KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
JON B. STREETER - #101970
MICHAEL H. PAGE - #154913
RAGESH K. TANGRI - #159477
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
CHRISTOPHER P. ISAAC
1300 I Street, N.W.
Washington, D.C. 20005-3314
Telephone: (202) 408-4000
Facsimile: (202) 408-4400

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	C 01 1640 JL Case No. **COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NO. 6,185,683 B1** **DEMAND FOR JURY TRIAL**

Plaintiff INTERTRUST TECHNOLOGIES CORPORATION (hereafter "InterTrust") hereby complains of Defendant MICROSOFT CORPORATION (hereafter "Microsoft"), and alleges as follows:

JURISDICTION AND VENUE

1. This action for patent infringement arises under the patent laws of the United States, Title 35, United States Code, more particularly 35 U.S.C. §§ 271 and 281.

2. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(c) and 1400(b).

THE PARTIES

4. Plaintiff InterTrust is a Delaware corporation with its principal place of business at 4750 Patrick Henry Drive, Santa Clara, California.

5. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft is a Washington Corporation with its principal place of business at One Microsoft Way, Redmond, Washington.

6. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft does business in this judicial district and has committed and is continuing to commit acts of infringement in this judicial district.

7. InterTrust is the owner of United States Patent No. 6,185,683 B1, entitled "Trusted and secure techniques, systems and methods for item delivery and execution" ("the '683 patent"), duly and lawfully issued on February 6, 2001. A copy of the '683 patent is attached hereto as Exhibit A.

CLAIM FOR RELIEF

8. InterTrust hereby incorporates by reference paragraphs 1-7 as if restated herein.

9. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

10. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '683 patent under § 271(a) by making, using, selling, and offering for sale digital rights management software incorporating inventions claimed in the '683 patent. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(a) will continue unless enjoined by this Court.

11. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '683 patent under

§ 271(a), thereby inducing infringement of the '683 patent under § 271(b). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(b) will continue unless enjoined by this Court.

12. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '683 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(c) will continue unless enjoined by this Court.

13. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '683 patent in the manner described above in paragraphs 10 through 12, and will continue to do so unless enjoined by this Court.

14. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, InterTrust prays for relief as follows:

A. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(a);

B. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '683 patent under 35 U.S.C. § 271(a);

C. That Microsoft be adjudged to have contributorily infringed the '683 patent under 35 U.S.C. § 271(c);

D. That Microsoft be adjudged to have willfully infringed the '683 patent under 35 U.S.C. §§ 271(a), (b), and (c);

E. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '683 patent;

F. That this Court award damages to compensate InterTrust for Microsoft's infringement, as well as enhanced damages, pursuant to 35 U.S.C. § 284;

G. That this Court adjudge this case to be exceptional and award reasonable attorney's fees to InterTrust pursuant to 35 U.S.C. § 285

H. That this Court assess pre-judgment and post-judgment interest and costs against Microsoft, and award such interest and costs to InterTrust, pursuant to 35 U.S.C. § 284; and

I. That InterTrust have such other and further relief as the Court may deem proper.

Dated: April 26, 2001

KEKER & VAN NEST, LLP

By:____________________________
JOHN W. KEKER
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

DEMAND FOR JURY TRIAL

Plaintiff InterTrust herby demands a trial by jury as to all issues triable by jury, specifically including, but not limited to, the issue of infringement of United States Patent No. 6,185,683 B1.

Dated: April 26, 2001

KEKER & VAN NEST, LLP

By: ________________
JOHN W. KEKER
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
JON B. STREETER - #101970
MICHAEL H. PAGE - #154913
RAGESH K. TANGRI - #159477
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
CHRISTOPHER P. ISAAC
1300 I Street, N.W.
Washington, D.C. 20005-3314
Telephone: (202) 408-4000
Facsimile: (202) 408-4400

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01 1640 JL **FIRST AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 6,185,683 B1 AND 6,253,193 B1** **DEMAND FOR JURY TRIAL**

Plaintiff INTERTRUST TECHNOLOGIES CORPORATION (hereafter "InterTrust") hereby complains of Defendant MICROSOFT CORPORATION (hereafter "Microsoft"), and alleges as follows:

JURISDICTION AND VENUE

1. This action for patent infringement arises under the patent laws of the United States, Title 35, United States Code, more particularly 35 U.S.C. §§ 271 and 281.

2. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(c) and 1400(b).

THE PARTIES

4. Plaintiff InterTrust is a Delaware corporation with its principal place of business at 4750 Patrick Henry Drive, Santa Clara, California.

5. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft is a Washington Corporation with its principal place of business at One Microsoft Way, Redmond, Washington.

6. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft does business in this judicial district and has committed and is continuing to commit acts of infringement in this judicial district.

7. InterTrust is the owner of United States Patent No. 6,185,683 B1, entitled "Trusted and secure techniques, systems and methods for item delivery and execution" ("the '683 patent"), duly and lawfully issued on February 6, 2001. A copy of the '683 patent is attached hereto as Exhibit A.

8. InterTrust is the owner of United States Patent No. 6,253,193 B1, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '193 patent"), duly and lawfully issued on June 26, 2001. A copy of the '193 patent is attached hereto as Exhibit B.

FIRST CLAIM FOR RELIEF

9. InterTrust hereby incorporates by reference paragraphs 1-7 as if restated herein.

10. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

11. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '683 patent under § 271(a) by making, using, selling, and offering for sale digital rights management software incorporating inventions claimed in the '683 patent.

InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(a) will continue unless enjoined by this Court.

12. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '683 patent under § 271(a), thereby inducing infringement of the '683 patent under § 271(b). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(b) will continue unless enjoined by this Court.

13. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '683 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(c) will continue unless enjoined by this Court.

14. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '683 patent in the manner described above in paragraphs 11 through 13, and will continue to do so unless enjoined by this Court.

15. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SECOND CLAIM FOR RELIEF

16. InterTrust hereby incorporates by reference paragraphs 1-6 and 8 as if restated herein.

17. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

18. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '193 patent under § 271(a) by making, using, selling, and offering for sale digital rights management software incorporating inventions claimed in the '193 patent.

InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(a) will continue unless enjoined by this Court.

19. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '193 patent under § 271(a), thereby inducing infringement of the '193 patent under § 271(b). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(b) will continue unless enjoined by this Court.

20. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '193 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(c) will continue unless enjoined by this Court.

21. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '193 patent in the manner described above in paragraphs 18 through 20, and will continue to do so unless enjoined by this Court.

22. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, InterTrust prays for relief as follows:

A. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(a);

B. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '683 patent under 35 U.S.C. § 271(a);

C. That Microsoft be adjudged to have contributorily infringed the '683 patent under

35 U.S.C. § 271(c);

D. That Microsoft be adjudged to have willfully infringed the '683 patent under 35 U.S.C. §§ 271(a), (b), and (c);

E. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '683 patent;

F. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(a);

G. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '193 patent under 35 U.S.C. § 271(a);

H. That Microsoft be adjudged to have contributorily infringed the '193 patent under 35 U.S.C. § 271(c);

I. That Microsoft be adjudged to have willfully infringed the '193 patent under 35 U.S.C. §§ 271(a), (b), and (c);

J. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '193 patent;

K. That this Court award damages to compensate InterTrust for Microsoft's infringement, as well as enhanced damages, pursuant to 35 U.S.C. § 284;

L. That this Court adjudge this case to be exceptional and award reasonable attorney's fees to InterTrust pursuant to 35 U.S.C. § 285;

M. That this Court assess pre-judgment and post-judgment interest and costs against Microsoft, and award such interest and costs to InterTrust, pursuant to 35 U.S.C. § 284; and

N. That InterTrust have such other and further relief as the Court may deem proper.

Dated: June 26, 2001

KEKER & VAN NEST, LLP

By: James M Emery for

JOHN W. KEKER
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

DEMAND FOR JURY TRIAL

Plaintiff InterTrust herby demands a trial by jury as to all issues triable by jury, specifically including, but not limited to, the issue of infringement of United States Patent No. 6,185,683 B1 and the issue of infringement of United States Patent No. 6,253,193 B1.

Dated: June 26, 2001

KEKER & VAN NEST, LLP

By: James M Emery for

JOHN W. KEKER
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

PROOF OF SERVICE

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

On June 26, 2001, I served the following document(s):

FIRST AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 6,185,683 B1 AND 6,253,193 B1

DEMAND FOR JURY TRIAL

XX by regular **UNITED STATES MAIL** by placing a true and correct copy in a sealed envelope addressed as shown below. I am readily familiar with the practice of Keker & Van Nest, LLP for collection and processing of correspondence for mailing. According to that practice, items are deposited with the United States Postal Service at San Francisco, California on that same day with postage thereon fully prepaid. I am aware that, on motion of the party served, service is presumed invalid if the postal cancellation date or the postage meter date is more than one day after the date of deposit for mailing stated in this affidavit.

Select by **COURIER**, by placing a true and correct copy in a sealed envelope addressed as shown below, and dispatching a messenger from [MESSENGER COMPANY], whose address is [MESSENGER COMPANY ADDRESS], with instructions to hand-carry the above and make delivery to the following during normal business hours, by leaving a true copy thereof with the person whose name is shown or the person authorized to accept courier deliveries on behalf of the addressee.

via Courier
Eric L. Wesenberg, Esq.
Mark R. Weinstein, Esq.
Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park CA 94025
Fax: 650-614-74401

via U.S. Mail
John D. Vandenberg, Esq.
James E. Geringer, Esq.
Klarquist Sparkman Campbell, et al.
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland OR 97204
Fax: 503-228-9446

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on June 26, 2001, at San Francisco, California.

Maria Li Mangiapane
MARIA LI-MANGIAPANE

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
JON B. STREETER - #101970
MICHAEL H. PAGE - #154913
RAGESH K. TANGRI - #159477
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
CHRISTOPHER P. ISAAC
1300 I Street, N.W.
Washington, D.C. 20005-3314
Telephone: (202) 408-4000
Facsimile: (202) 408-4400

Attomeys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION,
a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

Case No. C 01 1640 JL

SECOND AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 6,185,683 B1 AND 6,253,193 B1; 5,920,861; 5,940, 504

DEMAND FOR JURY TRIAL

Plaintiff INTERTRUST TECHNOLOGIES CORPORATION (hereafter "InterTrust") hereby complains of Defendant MICROSOFT CORPORATION (hereafter "Microsoft"), and alleges as follows:

JURISDICTION AND VENUE

1. This action for patent infringement arises under the patent laws of the United States, Title 35, United States Code, more particularly 35 U.S.C. §§ 271 and 281.

2. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(c) and 1400(b).

THE PARTIES

4. Plaintiff InterTrust is a Delaware corporation with its principal place of business at 4750 Patrick Henry Drive, Santa Clara, California.

5. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft is a Washington Corporation with its principal place of business at One Microsoft Way, Redmond, Washington.

6. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft does business in this judicial district and has committed and is continuing to commit acts of infringement in this judicial district.

7. InterTrust is the owner of United States Patent No. 6,185,683 B1, entitled "Trusted and secure techniques, systems and methods for item delivery and execution" ("the '683 patent"), duly and lawfully issued on February 6, 2001. A copy of the '683 patent is attached hereto as Exhibit A.

8. InterTrust is the owner of United States Patent No. 6,253,193 B1, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '193 patent"), duly and lawfully issued on June 26, 2001. A copy of the '193 patent is attached hereto as Exhibit B.

9. InterTrust is the owner of United States Patent No. 5,940,504, entitled "Licensing management system and method in which datagrams including an addressee of a licensee and indicative of use of a licensed product are sent from the licensee's site" ("the '504 patent"), duly and lawfully issued on August 17, 1999. A copy of the '504 patent is attached hereto as Exhibit C.

10. InterTrust is the owner of United States Patent No. 5,920,861, entitled

"Techniques for defining, using and manipulating rights management data structures" ("the '861 patent"), duly and lawfully issued on July 6, 1999. A copy of the '861 patent is attached hereto as Exhibit D.

FIRST CLAIM FOR RELIEF

11. InterTrust hereby incorporates by reference paragraphs 1-7 as if restated herein.

12. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

13. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing thc '683 patent under § 271(a) by making and using systems incorporating Windows Media Player Versions 7 and 8. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '683 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(a) will continue unless enjoined by this Court.

14. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '683 patent under § 271(a), thereby inducing infringement of the '683 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(b) will continue unless enjoined by this Court.

15. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '683 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(c) will continue unless enjoined by this Court.

16. InterTrust is informed and believes, and on that basis alleges, that Microsoft is

willfully infringing the '683 patent in the manner described above in paragraphs 13 through 15, and will continue to do so unless enjoined by this Court.

17. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed..

SECOND CLAIM FOR RELIEF

18. InterTrust hereby incorporates by reference paragraphs 1-6 and 8 as if restated herein.

19. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

20. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '193 patent under § 271(a) by using Windows Media Player Versions 7 and 8. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '193 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(a) will continue unless enjoined by this Court.

21. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '193 patent under § 271(a), thereby inducing infringement of the '683 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(b) will continue unless enjoined by this Court.

22. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '193 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing

use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(c) will continue unless enjoined by this Court.

23. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '193 patent in the manner described above in paragraphs 20 through 22, and will continue to do so unless enjoined by this Court.

24. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

THIRD CLAIM FOR RELIEF

25. InterTrust hereby incorporates by reference paragraphs 1-6 and 9 as if restated herein.

26. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

27. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '504 patent under § 271(a) by Microsoft's use of the Product Activation feature of Microsoft XP and other Microsoft products. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '504 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '504 patent under §271(a) will continue unless enjoined by this Court.

28. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '504 patent under § 271(a), thereby inducing infringement of the '504 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of the Product Activation feature of Windows XP and

other Microsoft products. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '504 patent under §271(b) will continue unless enjoined by this Court.

29. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '504 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including the Product Activation feature of Windows XP and other Microsoft products. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '504 patent under §271(c) will continue unless enjoined by this Court.

30. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '504 patent in the manner described above in paragraphs 27 through 29, and will continue to do so unless enjoined by this Court.

31. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

FOURTH CLAIM FOR RELIEF

32. InterTrust hereby incorporates by reference paragraphs 1-6 and 10 as if restated herein.

33. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

34. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '861 patent under § 271(a) by making, using, selling, and offering for sale digital rights management software incorporating inventions claimed in the '861 patent, including but not limited to the Digital Asset Server and Microsoft Reader. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '861 patent under §

271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under §271(a) will continue unless enjoined by this Court.

35. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '861 patent under § 271(a), thereby inducing infringement of the '861 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of Digital Asset Server and Microsoft Reader. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under §271(b) will continue unless enjoined by this Court.

36. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '861 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including but not limited to the Digital Asset Server and Microsoft Reader. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under §271(c) will continue unless enjoined by this Court.

37. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '861 patent in the manner described above in paragraphs 32 through 34, and will continue to do so unless enjoined by this Court.

38. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, InterTrust prays for relief as follows:

A. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(a);

B. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '683 patent under 35 U.S.C. § 271(a);

C. That Microsoft be adjudged to have contributorily infringed the '683 patent under 35 U.S.C. § 271(c);

D. That Microsoft be adjudged to have willfully infringed the '683 patent under 35 U.S.C. §§ 271(a), (b), and (c);

E. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '683 patent;

F. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(a);

G. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '193 patent under 35 U.S.C. § 271(a);

H. That Microsoft be adjudged to have contributorily infringed the '193 patent under 35 U.S.C. § 271(c);

I. That Microsoft be adjudged to have willfully infringed the '193 patent under 35 U.S.C. §§ 271(a), (b), and (c);

J. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '193 patent;

K. That Microsoft be adjudged to have infringed the '504 patent under 35 U.S.C. § 271(a);

L. That Microsoft be adjudged to have infringed the '504 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '504 patent under 35 U.S.C. § 271(a);

M. That Microsoft be adjudged to have contributorily infringed the '504 patent under 35 U.S.C. § 271(c);

N. That Microsoft be adjudged to have willfully infringed the '504 patent under 35 U.S.C. §§ 271(a), (b), and (c);

O. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '504 patent;

P. That this Court award damages to compensate InterTrust for Microsoft's infringement, as well as enhanced damages, pursuant to 35 U.S.C. § 284;

Q. That this Court adjudge this case to be exceptional and award reasonable attorney's fees to InterTrust pursuant to 35 U.S.C. § 285;

R. That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. § 271(a);

S. That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '861 patent under 35 U.S.C. § 271(a);

T. That Microsoft be adjudged to have contributorily infringed the '861 patent under 35 U.S.C. § 271(c);

U. That Microsoft be adjudged to have willfully infringed the '861 patent under 35 U.S.C. §§ 271(a), (b), and (c);

V. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '861 patent;

W. That this Court assess pre-judgment and post-judgment interest and costs against Microsoft, and award such interest and costs to InterTrust, pursuant to 35 U.S.C. § 284; and

X. That InterTrust have such other and further relief as the Court may deem proper.

Dated: July 25, 2001

KEKER & VAN NEST, LLP

By: ______________________
JON B. STREETER
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

DEMAND FOR JURY TRIAL

Plaintiff InterTrust herby demands a trial by jury as to all issues triable by jury, specifically including, but not limited to, the issue of infringement of United States Patent Nos. 6,185,683 B1; 6,253,193 B1; 5,940,504; and 5,920,861.

Dated: July 25, 2001

KEKER & VAN NEST, LLP

By:________________________
JON B. STREETER
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

PROOF OF SERVICE

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

On July 26, 2001, I served the following document(s):

SECOND AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 6,185,683 B1 AND 6,253,193 B1; 5,920,861; 5,940, 504

☑ by COURIER, by placing a true and correct copy in a sealed envelope addressed as shown below, and dispatching a messenger from FIRST LEGAL with instructions to hand-carry the above and make delivery to the following during normal business hours, by leaving a true copy thereof with the person whose name is shown or the person authorized to accept courier deliveries on behalf of the addressee.

Eric L. Wesenberg, Esq.
Mark R. Weinstein, Esq.
Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94015

☑ by FEDERAL EXPRESS, by placing a true and correct copy in a sealed envelope addressed as shown below. I am readily familiar with the practice of Keker & Van Nest, LLP for correspondence for delivery by FedEx Corporation. According to that practice, items are retrieved daily by a FedEx Corporation employee for overnight delivery.

John D. Vandenberg, Esq.
James E. Geringer, Esq.
Steven R. Alexander, Esq.
Klarquist Sparkman Campbell Leigh & Whinston
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on July 26, 2001, at San Francisco, California.

Maria Li Mangiapane
MARIA LI MANGIAPANE

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG (admitted *Pro Hac Vice*)
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington Corporation,

Defendant.

CASE NO: C 01-1640 SBA

MICROSOFT CORPORATION'S ANSWER TO THE SECOND AMENDED COMPLAINT

Defendant Microsoft Corporation ("Microsoft") answers the Second Amended Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

1. Microsoft admits that the Second Amended Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Second Amended Complaint.

2. Microsoft admits that the Second Amended Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Second Amended Complaint.

4. Upon information and belief, Microsoft admits the allegations of paragraph 4 of the Second Amended Complaint.

5. Microsoft admits the allegations of paragraph 5 of the Second Amended Complaint.

6. Microsoft admits, for purposes of this action only, that it transacts business in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the Second Amended Complaint.

7. Microsoft admits that on its face the title page of U.S. Patent No. 6,185,683 B1 ("the '683 Patent") states that it was issued February 6, 2001, is entitled "Trusted and secure techniques, systems and methods for item delivery and execution," and lists "InterTrust Technologies Corp." as the assignee. Microsoft admits that a copy of the '683 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft, but denies that such copy was full and complete insofar as it did not include any material purportedly incorporated by reference therein. Microsoft denies that the '683 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 7 of the Second Amended Complaint.

8. Microsoft admits that on its face the title page of U.S. Patent No. 6,253,193 B1 ("the '193 Patent") states that it was issued June 26, 2001, is entitled "Systems and methods for the secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corporation" as the assignee. Microsoft admits that a copy of text associated with the '193 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft, but denies that such copy was full and complete as it did not include, among other

things, any of the drawings or figures. Microsoft further denies such copy was full and complete insofar as it did not include any material purportedly incorporated by reference therein. Microsoft denies that the '193 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 8 of the Second Amended Complaint.

9. Microsoft admits that on its face the title page of U.S. Patent No. 5,940,504 ("the '504 Patent") states that it was issued August 17, 1999 and is entitled "Licensing management system and method in which datagrams including an addressee of a licensee and indicative of use of a licensed product are sent from the licensee's site." Microsoft admits that a copy of the '504 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft. Microsoft denies that the '504 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 9 of the Second Amended Complaint.

10. Microsoft admits that on its face the title page of U.S. Patent No. 5,920,861 ("the '861 Patent") states that it was issued July 6, 1999, is entitled "Techniques for defining, using and manipulating rights management data structures," and lists "InterTrust Technologies Corp." as the assignee. Microsoft admits that a copy of the '861 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft, but denies that such copy was full and complete insofar as it did not include any material purportedly incorporated by reference therein. Microsoft denies that the '861 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 10 of the Second Amended Complaint.

11. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Second Amended Complaint, as if fully restated herein.

12. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 12 of the Second Amended Complaint.

13. Microsoft denies any and all allegations of paragraph 13 of the Second

Amended Complaint.

14. Microsoft denies any and all allegations of paragraph 14 of the Second Amended Complaint.

15. Microsoft denies any and all allegations of paragraph 15 of the Second Amended Complaint.

16. Microsoft denies any and all allegations of paragraph 16 of the Second Amended Complaint.

17. Microsoft denies any and all allegations of paragraph 17 of the Second Amended Complaint.

18. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 8 of the Second Amended Complaint, as if fully restated herein.

19. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281.. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 19 of the Second Amended Complaint.

20. Microsoft denies any and all allegations of paragraph 20 of the Second Amended Complaint.

21. Microsoft denies any and all allegations of paragraph 21 of the Second Amended Complaint.

22. Microsoft denies any and all allegations of paragraph 22 of the Second Amended Complaint.

23. Microsoft denies any and all allegations of paragraph 23 of the Second Amended Complaint.

24. Microsoft denies any and all allegations of paragraph 24 of the Second Amended Complaint.

25. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 9 of the Second Amended Complaint, as if fully restated herein.

///

26. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 26 of the Second Amended Complaint.

27. Microsoft denies any and all allegations of paragraph 27 of the Second Amended Complaint.

28. Microsoft denies any and all allegations of paragraph 28 of the Second Amended Complaint.

29. Microsoft denies any and all allegations of paragraph 29 of the Second Amended Complaint.

30. Microsoft denies any and all allegations of paragraph 30 of the Second Amended Complaint.

31. Microsoft denies any and all allegations of paragraph 31 of the Second Amended Complaint.

32. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 10 of the Second Amended Complaint, as if fully restated herein.

33. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 33 of the Second Amended Complaint.

34. Microsoft denies any and all allegations of paragraph 34 of the Second Amended Complaint.

35. Microsoft denies any and all allegations of paragraph 35 of the Second Amended Complaint.

36. Microsoft denies any and all allegations of paragraph 36 of the Second Amended Complaint.

37. Microsoft denies any and all allegations of paragraph 37 of the Second Amended Complaint.

38. Microsoft denies any and all allegations of paragraph 38 of the Second Amended Complaint.

AFFIRMATIVE AND OTHER DEFENSES

. Further answering the Second Amended Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patents

1. Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,185,683 B1 ("the '683 Patent"), U.S. Patent No. 6,253,193 B1 ("the '193 Patent"), U.S. Patent No. 5,940,504 ("the '504 Patent") or U.S. Patent No. 5,920,861 ("the '861 Patent"), and is not liable for infringement thereof.

2. Any and all Microsoft products or actions that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '683 Patent, the '193 Patent, the '504 Patent or the '861 Patent.

Second Defense: Invalidity of the Asserted Patents

3. On information and belief, the '683 Patent, the '193 Patent, the '504 Patent and the '861 Patent are invalid for failing to comply with the provisions of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailability of Relief

4. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 271(b) and is not entitled to any alleged damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent or the '861 Patent.

Fourth Defense: Unavailability of Relief

5. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent, and any alleged infringement thereof.

Fifth Defense: Unavailability of Relief

6. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any damages.

Sixth Defense: Prosecution History Estoppel

7. Plaintiff's alleged causes of action for patent infringement are barred under the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

8. Plaintiff has dedicated to the public all methods, apparatus, and products disclosed in the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent, but not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture By/For United States Government

9. To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

10. To the extent that any of Plaintiff's allegations of infringement are premised on the alleged use, sale, or offer for sale of products that were manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft to or by a licensee of InterTrust, such allegations are barred pursuant to license.

Tenth Defense: Acquiescence

11. Plaintiff has acquiesced in at least those acts of Microsoft that are alleged to infringe the '861 Patent, the '683 Patent, and the '193 Patent.

Eleventh Defense: Laches

12. Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A. The Court enter judgment against InterTrust on, and dismiss with prejudice, any and all claims of the Second Amended Complaint;

B. The Court award to Microsoft its reasonable costs and attorneys' fees; and

C. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

DATED: August 29, 2001

By:

ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
Microsoft Corporation

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG (admitted *Pro Hac Vice*)
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington Corporation,

Defendant.

CASE NO: C 01-1640 SBA

MICROSOFT CORPORATION'S FIRST AMENDED ANSWER AND COUNTERCLAIMS TO THE SECOND AMENDED COMPLAINT

Defendant Microsoft Corporation ("Microsoft") answers the Second Amended Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

1. Microsoft admits that the Second Amended Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft

in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Second Amended Complaint.

2. Microsoft admits that the Second Amended Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Second Amended Complaint.

4. Upon information and belief, Microsoft admits the allegations of paragraph 4 of the Second Amended Complaint.

5. Microsoft admits the allegations of paragraph 5 of the Second Amended Complaint.

6. Microsoft admits, for purposes of this action only, that it transacts business in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the Second Amended Complaint.

7. Microsoft admits that on its face the title page of U.S. Patent No. 6,185,683 B1 ("the '683 Patent") states that it was issued February 6, 2001, is entitled "Trusted and secure techniques, systems and methods for item delivery and execution," and lists "InterTrust Technologies Corp." as the assignee. Microsoft admits that a copy of the '683 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft, but denies that such copy was full and complete insofar as it did not include any material purportedly incorporated by reference therein. Microsoft denies that the '683 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 7 of the Second Amended Complaint.

8. Microsoft admits that on its face the title page of U.S. Patent No. 6,253,193 B1 ("the '193 Patent") states that it was issued June 26, 2001, is entitled "Systems and methods for the secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corporation" as the assignee. Microsoft admits that a copy of text associated with

the '193 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft, but denies that such copy was full and complete as it did not include, among other things, any of the drawings or figures. Microsoft further denies such copy was full and complete insofar as it did not include any material purportedly incorporated by reference therein. Microsoft denies that the '193 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 8 of the Second Amended Complaint.

9. Microsoft admits that on its face the title page of U.S. Patent No. 5,940,504 ("the '504 Patent") states that it was issued August 17, 1999 and is entitled "Licensing management system and method in which datagrams including an addressee of a licensee and indicative of use of a licensed product are sent from the licensee's site." Microsoft admits that a copy of the '504 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft. Microsoft denies that the '504 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 9 of the Second Amended Complaint.

10. Microsoft admits that on its face the title page of U.S. Patent No. 5,920,861 ("the '861 Patent") states that it was issued July 6, 1999, is entitled "Techniques for defining, using and manipulating rights management data structures," and lists "InterTrust Technologies Corp." as the assignee. Microsoft admits that a copy of the '861 Patent was attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft, but denies that such copy was full and complete insofar as it did not include any material purportedly incorporated by reference therein. Microsoft denies that the '861 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 10 of the Second Amended Complaint.

11. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Second Amended Complaint, as if fully restated herein.

12. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft

denies any and all remaining allegations of paragraph 12 of the Second Amended Complaint.

13. Microsoft denies any and all allegations of paragraph 13 of the Second Amended Complaint.

14. Microsoft denies any and all allegations of paragraph 14 of the Second Amended Complaint.

15. Microsoft denies any and all allegations of paragraph 15 of the Second Amended Complaint.

16. Microsoft denies any and all allegations of paragraph 16 of the Second Amended Complaint.

17. Microsoft denies any and all allegations of paragraph 17 of the Second Amended Complaint.

18. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 8 of the Second Amended Complaint, as if fully restated herein.

19. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 19 of the Second Amended Complaint.

20. Microsoft denies any and all allegations of paragraph 20 of the Second Amended Complaint.

21. Microsoft denies any and all allegations of paragraph 21 of the Second Amended Complaint.

22. Microsoft denies any and all allegations of paragraph 22 of the Second Amended Complaint.

23. Microsoft denies any and all allegations of paragraph 23 of the Second Amended Complaint.

24. Microsoft denies any and all allegations of paragraph 24 of the Second Amended Complaint.

25. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 9 of the Second Amended Complaint, as if fully restated herein.

26. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 26 of the Second Amended Complaint.

27. Microsoft denies any and all allegations of paragraph 27 of the Second Amended Complaint.

28. Microsoft denies any and all allegations of paragraph 28 of the Second Amended Complaint.

29. Microsoft denies any and all allegations of paragraph 29 of the Second Amended Complaint.

30. Microsoft denies any and all allegations of paragraph 30 of the Second Amended Complaint.

31. Microsoft denies any and all allegations of paragraph 31 of the Second Amended Complaint.

32. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 10 of the Second Amended Complaint, as if fully restated herein.

33. Microsoft admits that the Second Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 33 of the Second Amended Complaint.

34. Microsoft denies any and all allegations of paragraph 34 of the Second Amended Complaint.

35. Microsoft denies any and all allegations of paragraph 35 of the Second Amended Complaint.

36. Microsoft denies any and all allegations of paragraph 36 of the Second Amended Complaint.

37. Microsoft denies any and all allegations of paragraph 37 of the Second Amended Complaint.

38. Microsoft denies any and all allegations of paragraph 38 of the Second Amended Complaint.

AFFIRMATIVE AND OTHER DEFENSES

Further answering the Second Amended Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patents

1. Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,185,683 B1 ("the '683 Patent"), U.S. Patent No. 6,253,193 B1 ("the '193 Patent"), U.S. Patent No. 5,940,504 ("the '504 Patent") or U.S. Patent No. 5,920,861 ("the '861 Patent"), and is not liable for infringement thereof.

2. Any and all Microsoft products or actions that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '683 Patent, the '193 Patent, the '504 Patent or the '861 Patent.

Second Defense: Invalidity of the Asserted Patents

3. On information and belief, the '683 Patent, the '193 Patent, the '504 Patent and the '861 Patent are invalid for failing to comply with the provisions of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailabilitv of Relief

4. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 271(b) and is not entitled to any alleged damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent or the '861 Patent.

Fourth Defense: Unavailability of Relief

5. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to

providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent, and any alleged infringement thereof.

Fifth Defense: Unavailability of Relief

6. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any damages.

Sixth Defense: Prosecution History Estoppel

7. Plaintiff's alleged causes of action for patent infringement are barred under the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

8. Plaintiff has dedicated to the public all methods, apparatus, and products disclosed in the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent, but not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture By/For United States Government

9. To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

10. To the extent that any of Plaintiff's allegations of infringement are premised on the alleged use, sale, or offer for sale of products that were manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft to or by a licensee of InterTrust, such allegations are barred pursuant to license.

Tenth Defense: Acquiescence

11. Plaintiff has acquiesced in at least those acts of Microsoft that are alleged to infringe the '861 Patent, the '683 Patent, and the '193 Patent.

Eleventh Defense: Laches

12. Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

13. The '861 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '861 Patent, set forth below.

COUNTERCLAIMS

COUNT I - DECLARATORY JUDGMENT OF NONINFRINGEMENT

1. This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, et seq. This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

2. Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

3. Upon information and belief, Plaintiff /Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

4. InterTrust purports to be the owner of U.S. Patent Nos. 6,185,683 B1 ("the '683 Patent"), 6,253,193 B1 ("the '193 Patent"), 5,940,504 ("the '504 Patent"), and 5,920,861 ("the '861 Patent").

5. InterTrust alleges that Microsoft has infringed the '683 Patent, the '193 Patent, the '504 Patent, and the '861 Patent.

6. No Microsoft product has infringed, either directly or indirectly, any claim of the '683 Patent, the '193 Patent, the '504 Patent, or the '861 Patent, and Microsoft is not liable for infringement thereof.

///

7. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the infringement or noninfringement of the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent.

COUNT II - DECLARATORY JUDGMENT OF INVALIDITY OF THE '683 PATENT

8. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

9. The '683 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

10. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '683 Patent are valid or invalid.

COUNT III - DECLARATORY JUDGMENT OF INVALIDITY OF THE '193 PATENT

11. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

12. The '193 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

13. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '193 Patent are valid or invalid.

COUNT IV - DECLARATORY JUDGMENT OF INVALIDITY OF THE '504 PATENT

14. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

15. The '504 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

16. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '504 Patent are valid or invalid.

COUNT V - DECLARATORY JUDGMENT OF INVALIDITY OF THE '861 PATENT

17. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

18: The '861 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

19. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are valid or invalid.

COUNT VI - DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '861 PATENT

20. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

21. Claims 1-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, were not and are not entitled to benefit of any application filing date prior to February 25, 1997, under 35 U.S.C. § 120 or otherwise.

22. Exhibit A hereto is a reprint of an article entitled "Digibox: A Self-Protecting Container for Information Commerce." The article shown in Exhibit A (hereafter, "the Sibert article") was published in July 1995 in the Proceedings of the First USENIX Workshop on Electronic Commerce.

23. On information and belief, the content of pages 2-14 of Exhibit A was presented at a public conference in the United States in July 1995.

24. Exhibit B hereto is a copy of a page from an International Application published under the Patent Cooperation Treaty (PCT), bearing International Publication Number WO 96/27155.

25. On information and belief, International Application WO 96/27155 has, at all times since its filing date, been owned and controlled by InterTrust or its predecessors in interest.

26. International Application WO 96/27155 (hereafter "the WO 96/27155 (PCT) publication") was published on September 6, 1996.

27. United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8, 1999, from a continuation of an application filed on February 13, 1995.

28. The Sibert article is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, under 35 U.S.C. §§ 102(b), 103.

29. The WO 96/27155 (PCT) publication is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, under 35 U.S.C. §§ 102(a), 103.

30. The '987 Patent is prior art to claims 29-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, under 35 U.S.C. §§ 102(e), 103.

31. The Sibert article was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

32. The Sibert article was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

33. The WO 96/27155 (PCT) publication was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

34. The WO 96/27155 (PCT) publication was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

35. The '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804).

36. One or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the July 1995 publication of the Sibert article.

37. On information and belief, one or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the September 1996

publication of the WO 96/27155 (PCT) publication.

38. One or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the June 8, 1999 issuance of the '987 patent.

39. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the July 1995 publication of the Sibert article.

40. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

41. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the June 8, 1999 issuance of the '987 patent.

42. The applicants for the '861 Patent did not cite the Sibert article, the WO 96/27155 (PCT) publication, or the '987 Patent to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

43. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the Sibert article, the WO 96/27155 (PCT) publication, or the '987 Patent.

44. None of the Sibert article, the WO 96/27155 (PCT) publication, or the '987 Patent is merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

45. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

46. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication disclosed an embodiment of claim 1 of the '861 Patent

application (SN 08/805,804).

47. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the Sibert article was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

48. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the WO 96/27155 (PCT) publication was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

49. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

50. The '861 Patent is unenforceable due to the inequitable conduct of the '861 Patent applicants before the Patent and Trademark Office in connection with the '861 Patent application (SN 08/805,804).

51. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are enforceable.

COUNT VII - INFRINGEMENT OF U.S. PATENT NO. 6,049,671

52. Microsoft repeats and realleges paragraphs 2-3 of its Counterclaims, as if fully restated herein.

53. This Court has exclusive subject matter jurisdiction over Microsoft's cause of action for patent infringement under Title 28, United States Code, Sections 1331 and 1338, and under the patent laws of the United States, Title 35 of the United States Code.

54. U.S. Patent No. 6,049,671 ("the '671 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on April 11, 2000.

55. A true copy of the '671 Patent is attached as Exhibit C hereto, and is incorporated herein by reference.

56. Microsoft owns all right, title and interest in the '671 Patent.

57. InterTrust has had actual notice of the '671 Patent.

58. InterTrust has infringed one or more claims of the '671 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

59. InterTrust's infringement of the '671 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

COUNT VIII - INFRINGEMENT OF U.S. PATENT NO. 6,256,668

60. Microsoft repeats and realleges paragraphs 2-3 and 51 of its Counterclaims, as if fully restated herein.

61. U.S. Patent No. 6,256,668 B1 ("the '668 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on July 3, 2001.

62. A true copy of the '668 Patent is attached as Exhibit D hereto, and is incorporated herein by reference.

63. Microsoft owns all right, title and interest in the '668 Patent.

64. InterTrust has had actual notice of the '668 Patent.

65. InterTrust has infringed one or more claims of the '668 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

66. InterTrust's infringement of the '668 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A. The Court enter judgment against InterTrust on, and dismiss with prejudice, any and all claims of the Second Amended Complaint;

B. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '683 Patent;

C. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '193 Patent;

D. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '504 Patent;

E.. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '861 Patent;

F. The Court enter judgment declaring that the '683 Patent is invalid;

G. The Court enter judgment declaring that the '193 Patent is invalid;

H. The Court enter judgment declaring that the '504 Patent is invalid;

I. The Court enter judgment declaring that the '861 Patent is invalid;

J. The Court enter judgment that the '861 Patent is unenforceable due to inequitable conduct;

K. The Court enter judgment that InterTrust has infringed the '671 patent;

L. The Court enter judgment that InterTrust has infringed the '668 patent;

M. A permanent injunction prohibiting InterTrust, its officers, agents, servants, employees, and all persons in active concert or participation with them from infringing the '671 and '668 Patents;

N. An award against InterTrust of damages and attorney fees, pursuant to the provisions of 35 U.S.C §§ 284, 285.

O. An award to Microsoft of prejudgment interest and the costs of this action.

P. The Court award to Microsoft its reasonable costs and attorneys' fees; and

Q. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

///

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

DATED: September 17, 2001

By: Mark R. Weinstein

WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
Microsoft Corporation

Exhibit A

USENIX

The following paper was originally published in the
Proceedings of the First USENIX Workshop on Electronic Commerce
New York, New York, July 1995.

DigiBox: A Self-Protecting Container for Information Commerce

Olin Sibert, David Bernstein, and David Van Wie
Electronic Publishing Resources, Inc.
Sunnyvale, California

For more information about USENIX Association contact:
1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: http://www.usenix.org

The DigiBox:
A Self-Protecting Container for Information Commerce

Olin Sibert
David Bernstein
David Van Wie

Electronic Publishing Resources, Inc.
460 Oakmead Parkway
Sunnyvale, California
1 408 774 6100
info@epr.com

Abstract

Information Commerce is a business activity carried out among several parties in which information carries value and is treated as a product. The information may be content, it may be returned usage and marketing data, and it may be representative of financial transactions.

In each of these cases the information is valuable and must be kept secure and private. Traditional approaches secure the transmission of that information from one point to another; there are no persistent protections. Protection of all of these components of information commerce for all parties in a transaction value chain is necessary for a robust electronic infrastructure.

A prerequisite to such an environment is a cryptographically protected container for packaging information and controls that enforce information rights. This paper describes such a container, called the DigiBox™. EPR has submitted initial specifications for the DigiBox container to the ANSI IISP Electronic Publishing Task Force (EPUB) within the User/Content Provider Standards Working Group (WG4).

1 Introduction

As services and products in modern commerce increasingly take electronic form, traditional commerce is evolving into electronic commerce. This includes both creation and enforcement of various agreements between parties in an electronic commercial relationship. It also includes enforcing the rights of these parties with respect to the secure management of electronic content or services usage, billing, payment, and related activities.

To save money, to be competitive, and to be efficient [1,2], members of modern society will shortly be using new information technology tools that truly support electronic commerce. These tools provide for the flow of products and services through creators', providers', and users' hands. They enable the creation, negotiation, and enforcement of electronic agreements, including the evolution of controls that manage both the use and consequences of use of electronic content or services. In addition, these tools support "evolving" agreements that progressively reflect the requirements of further participants in a commercial model.

Participants in electronic commerce [3,4] will need rules and mechanisms such that:

1. Information providers can be assured that their content is used only in authorized ways;

2. Privacy rights of users of content are preserved; and

3. Diverse business models related to content can be electronically implemented.

The Internet and other information commerce infrastructures will require a management component that enforces such rules, ensuring a safe, coherent, fair, and productive community. This management component will be critical to the electronic highway's acceptance. Without rules to protect the rights of content providers and other electronic community members, the electronic highway will comprise nothing more than a collection of limited, disconnected applications.

Analysts have concluded that content will constitute the largest revenue-generating component of the information superhighway [5]. It is also clear that unfettered access to content requires that content providers be able to maintain control over literary or copyrighted assets. Many analysts conclude that this will be one of the key bottlenecks in the implementation and deployment of New Media.

2 Information Commerce and Digital Value Chains

Information commerce is often considered a wholly new concept, made possible only through the use of networks and computers. In fact, a robust information economy has existed for centuries, involving trafficking in physical *representations* of information such as books, newspapers, and so on. Because such commerce involves physical goods, there is a non-negligible floor to the cost of handling information goods. The new aspects of the electronic information economy are that the information itself is the entire product and that the product can be distributed at negligible marginal cost.

The traditional information economy in physical goods is publisher-centric, because creation of information goods—particularly low-cost goods—requires a substantial manufacturing investment. Figure 1 illustrates a simplified traditional information economy: physical goods flow from a publisher (manufacturer) to a customer, in response to orders and followed by payments. The author's relationship with the publisher may be more lightweight, but the author is nonetheless dependent on the publisher to report sales and make royalty payments in accordance with the author's contract. In addition, a financial institution provides payment processing and clearing services for all parties.

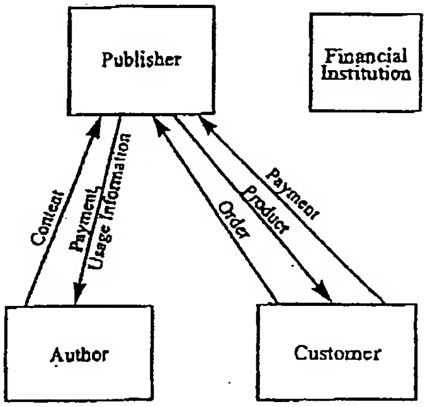

Figure 1. Traditional information economy.

Because of the flexibility afforded by electronic mechanisms, information commerce is evolving from indirect, advertiser-supported, mass-audience media to a new, niche-audience-oriented business model. In this system, members of the electronic community, with or without the economic support of advertising, pay providers directly for what they want to receive. Business-to-business purchasing is steadily evolving into a direct electronic ordering model.

Figure 2 illustrates the flexibility possible in new electronic information commerce models. Although there is still a role for publishers, this role no longer involves physical goods. Rather, the publisher is responsible for packaging and aggregating information goods and control information, then making them available to customers. Similar to a manufacturing/distribution/retail chain for physical goods, the electronic model permits information retailers, and even end customers, to repackage and redistribute different aggregations of information while ensuring that the appropriate control rules are maintained. A clearinghouse ensures that usage information and payments are provided directly to authors and publishers; the payments themselves are made through traditional financial institutions. Because control rules are associated with information, a variety of payment and other business models can be associated with the same content (e.g., *purchase* versus *pay-per-use*).

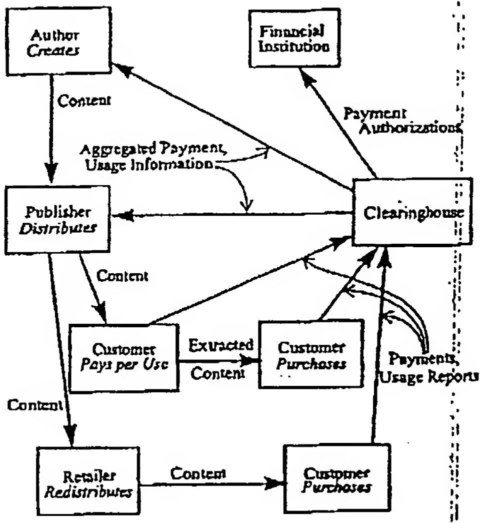

Figure 2. Electronic information economy.

The conversion from traditional commercial distribution channels requires key foundation technologies and results in a fundamental shift in existing infrastructures. This channel transformation will create a new electronic digital distribution industry. Digital distribution employing the DigiBox container architecture and its associated support environment, InterTrust™, can play a critical role in this transformation of the communication, media, and information technology markets.

2.1 Protecting All the Information in Information Commerce

The very properties that make "the net" attractive as a distribution medium—ease of manipulating information in electronic form—also appear to make these protections intractable. Addressing this dichotomy requires a paradigm shift in computer architecture to introduce the concept of a "secure processing" environment in which protected information can be manipulated without being subject to external tampering or disclosure. A prerequisite to such an environment is a cryptographically protected "container" for seamlessly packaging information and controls that enforce information use rights.

The DigiBox described by this paper is such a container.

The need for various information commerce computers and appliances to interoperate requires that this container format and its access methods be standardized. EPR has submitted initial specifications for the DigiBox container to the American National Standards Institute (ANSI) Information Infrastructure Standards Panel (IISP) through the Electronic Publishing Task Force (EPUB) in the User/Content Provider Standards Working Group (WG4).

The primary goal of information protection is to permit proprietors of digital information (i.e., the artists, writers, distributors, packagers, market researchers, etc.) to have the same type and degree of control present in the "paper world." Because digital information is intangible and easily duplicated, those rights are difficult to enforce with conventional information processing technology. Many types of rights (compensation, distribution, modification, etc.) are associated with the various elements of information commerce, and these information property rights take many forms. At a high level, there is the legal definition of "copyright," codified in U.S. law [6–9] and the Berne Convention. This gives copyright holders a legal right to control how copyrighted information is handled. In addition, various high-level rights are conferred by contractual arrangements between primary rightsholders and other parties.

For example, the protections needed for content elements incorporate the licensing provisions for the intellectual property rights of the content rightsholders. In a broader sense, these rights include control over several activities: the right to be compensated for use of the property; the right to control how content is distributed; the right to prevent modification of content by a distributor; "fair use" rights; the rights to the usage data, privacy rights of individuals, and so on.

In the realm of physical goods, these rights are enforced by a combination of legal and technical means. However, the technical means can be (and are) unsophisticated because the technology for violating rights is relatively expensive and time-consuming—in comparison to equivalent activities with respect to digital information. Photocopying a book or copying a video cassette is inherently more labor intensive and costly than copying a file. So, while defeating technical means of enforcement is (relatively) expensive, it can be done—and often the legal means to deter this are inadequate.

2.2 Information *Commerce*—Not Just Payment

Rights protection is also a fundamental aspect of commerce. Commerce is not just a way for two parties to pay each other for something. Rather, it is an extraordinarily rich web of relationships among parties that concerns payment, negotiation, control, advertising, reporting, auditing, and a variety of other activities. These activities are important aspects of the transaction relationships. Often the information carried in these reports, audits, and the like is highly valuable and highly confidential, perhaps even more valuable than the content that is the subject of the information commerce at hand. These activities too are performed and controlled in the "paper world" by legal and technical means, but there are no widely used models for their electronic equivalents.

Figure 3 shows some of the operations that could occur in true electronic commerce, using the Internet World-Wide Web [10] mechanisms as an example. Creators originate content and apply rules (e.g., "pay author $1.00/use") for its use. Distributors repackage content, applying additional rules (e.g., "pay $5.00 for the collection, then pay the creator," "report use of each item"). Users receive content and operate on it, generating billing reports and usage reports that are delivered to a clearinghouse and paid or summarized back for the originating parties. This structure is very rich and is capable of supporting many business models. There are multiple flows of information in many different directions amongst the parties involved in the transactions.

Another example is that of an advertiser (acting as distributor, or with a distributor). The advertiser might have a rule that offers a discount, or no charge at all, but only if the user views the advertisement and agrees to have that fact reported to the advertiser.

It is relatively simple to devise schemes for parties to pay each other electronically (for example, DigiCash [11], NetBill [12], Open Market [13], SNPP [14], NetCheque [15], First Virtual [16], etc.). Payment, however, constitutes only one—and perhaps the simplest one—of the means in which parties in commerce interact. All the other information commerce components must be accomplished with the same needs for security, privacy, and integrity. In fact, these aspects of electronic commerce, including rights protection, are strongly intertwined in the digital economy, because much digital commerce concerns information and innovative business models for information commerce.

3 Existing Approaches to Information Commerce

Information proprietors employ a variety of technological protection approaches today. These approaches are generally "point solutions," in that they protect a specific type of property in a specific context and enforce only specifically defined rights—typically only the right to compensation for use. Because the technologies are limited, the market is fragmented, and there are no general protection solutions.

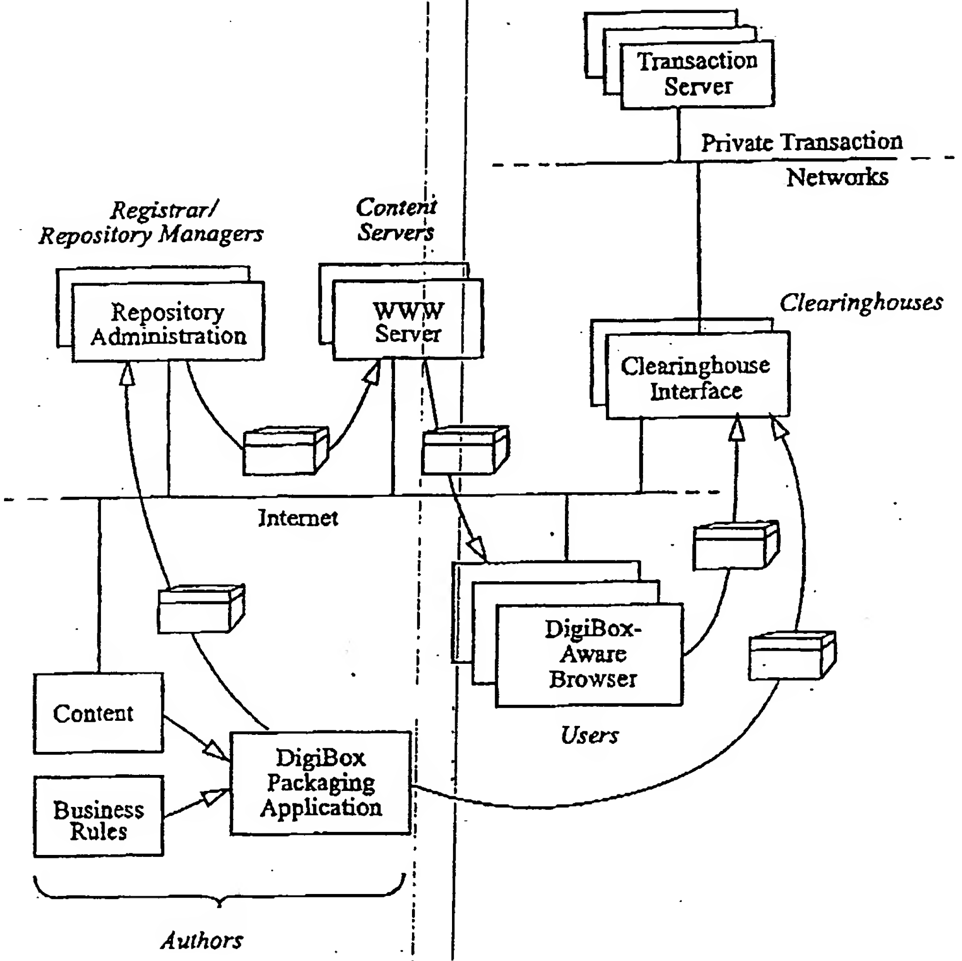

Figure 3. Multi-party Internet information commerce.

3.1 No Protection

Much digital property is distributed without any technological enforcement for property rights, on the assumption that legal means suffice. This approach works well enough for many low-value properties, but it has the disadvantage of raising the price to legitimate users who must pay for both their own and illegitimate use. In many cases, however, this cost is negligible, and no protection is an economically sound choice. Even for content that is free, however, a creator may wish to impose some rules for reporting or some access control. Of course, privacy rights of users will be a concern to many.

3.2 License Managers

For some valuable software properties, license managers are used. Because a software property is dynamic (executable), it is feasible to restrict it so that it functions properly only through interaction with a license manager process. In general, there is no protection of usage data in these schemes. In some cases this technique has been applied to content protection, but only with limited success [17, 18].

3.3 Cryptographic Unlock

Some static properties (fonts, for example; also some installable software) are protected by a simple "unlock" scheme: a purchaser makes a purchase, for example by telephone with a credit card, and receives a cryptographic key in return. This key can then be used to "unlock" one property from some widely distributed medium (e.g., CD-ROM or network download). This mechanism is relatively inflexible, and its inherently manual nature makes it expensive.

3.4 Billing Schemes

Various billing schemes (as mentioned above) permit purchase of information following what is essentially an electronic check or electronic credit draft model. These methods are suitable for conventional transactions, but not for the enormous volumes of (individually) very low-value transactions that would be generated using a complex digital property.

3.5 Secured Delivery

Various secured delivery systems (e.g., SSL [19], SHTTP [20]) share the same problems as cryptographic unlock, but in a network context. They are only point-to-point solutions, with the information (content, usage data, etc.) at each site being left unprotected once the delivery has occurred. Furthermore, they are inherently online systems: it is not practical to decouple the delivery of information from payment for its use.

4 Information Protection Architecture: InterTrust and DigiBox

EPR has produced the InterTrust Virtual Distribution Architecture to solve unmet, critical needs of electronic commerce. Almost any imaginable information transaction can be supported by InterTrust. A few examples include distribution of content (e.g., text, video, audio) over networks, selective release of data from a database, controlled release of sensitive information, and so on. InterTrust can also support the secure communication of private information such as EDI and electronic financial transactions, as well as delivery of the "back channel" marketing and usage data resulting from transactions.

DigiBox is a foundation technology within InterTrust. It provides a secure container to package information so that the information cannot be used except as provided by the rules and controls associated with the content. InterTrust rules and controls specify what types of content usage are permitted, as well as the consequences of usage such as reporting and payment.

Within InterTrust, DigiBox containers can enforce a "distributed electronic contract" for value-chain activities functioning within an electronic distribution environment. This unique approach underlies EPR's information metering and digital rights protection technology. Electronic commerce infrastructure participants can use InterTrust to substantially enhance their network, security, or payment method solutions.

The DigiBox is a container for both digital property (content) and controls. It is used in conjunction with a locally secured rights protection application (discussed further below) to make content available as governed by arbitrarily flexible controls.

The DigiBox container mechanism is implemented in a set of platform-independent class libraries that provide access to objects in the container and extensions to OpenDoc and OLE object technologies. DigiBox allows rights management components to be integrated with content in highly flexible and configurable control structures. Digi-

Box rights management components can be integrated with content in a single deliverable, or some or all of the components can be delivered independently. DigiBox rights management components enable true superdistribution [21] and can support virtually any network topology and any number of participants, including distributors, redistributors, information retailers, corporate content users, and consumers.

4.1 Content

The digital information in a DigiBox (one or more "properties") is information in any form. It may be mapped to a specific compound object format (e.g., OpenDoc, OLE, PDF), or may be application specific.

Further, it may be delivered in stream or other communication-oriented forms, not just in a file-like container.

4.2 Controls

Controls specify rules and consequences for operations on content. Controls are also delivered in a DigiBox, and the controls for a property may be delivered either with the property or independently. Controls are tied to properties by cryptographic means.

Because controls can be delivered with properties in a container, the DigiBox supports superdistribution.

4.3 Commerce

Commerce takes place governed by controls. This may involve metering, billing for use, reporting of usage, and so on. These operations take place locally in a secure environment, and they generate audit trails and reports that must be reported periodically to clearinghouses.

5 DigiBox Implementation

The DigiBox is a structure that can hold, in a protected manner, information commerce elements of all kinds: content, usage information, representation of financial transactions (e.g., electronic cash), and other digital elements of information commerce.

5.1 Container Logical Structure

Figure 4 shows the logical structure of properties and control sets in two containers. Container C_1 holds two properties, P_1 and P_2, and one control set, CS_1, that applies to property P_1; container C_2 contains two control sets and no properties. As shown in the example, each of these elements has a title attribute to provide a human-readable description of the element and, for control sets, an attribute indicating to what other elements the control set applies.

A control set specifies rules and consequences, such as pricing, reporting, and so on, for the properties to which it applies. A user holding just this container could use (e.g., view, print) content from P_1—though only as specified by CS_1. Because there is no control set applying to P_2 in that container, P_2 would not be usable in any way.

A user holding both containers could use property P_2, as specified by CS_2, and in addition has the choice of whether to designate CS_1 or CS_3 when using P_1. CS_3, which describes itself as "discount," is likely to be the user's preferred choice.

The DigiBox includes several elements: organizational structures, properties, controls, and supporting data items. Almost all the information in a DigiBox is encrypted, as described below, and access to the encrypted form is provided through a storage manager as appropriate, depending on how the DigiBox is delivered (e.g., as a file or as a data stream).

5.2 Container Physical Structure

Figure 5 is a schematic picture illustrating the physical structure of a DigiBox container. (Some elements have been omitted for clarity.) It begins with a *container header* structure containing descriptive and organizational information about the container. Part of the container header is encrypted (both for secrecy and for integrity protection); the rest is public organizational informa-

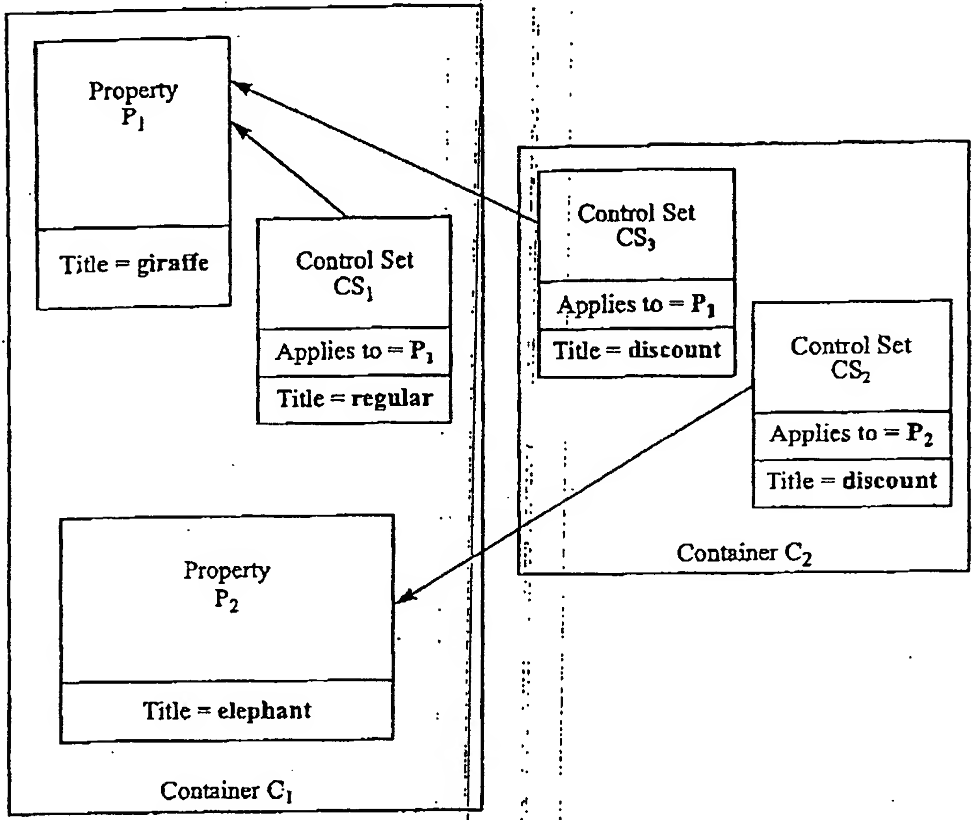

Figure 4. Container logical structure.

tion. The header is followed by additional container-wide structures such as the *transport key block (TKB)* and the *container table of contents (TOC)*, some of which are encrypted and others not.

These organizational elements are followed by the structures defining the container's content (e.g., *properties* and *control sets*). As shown in the figure, a property is represented by a *property header*, *property attributes*, and data blocks composing the property. As shown, the header is encrypted and the attributes are not; the data blocks may be wholly or partly encrypted, or not at all, depending on security requirements.

The figure shows an example property consisting of a multimedia property formed from a pair of synchronized data streams for audio and video. In this example, each video block is mostly unencrypted so that access can be rapid while still maintaining reasonable security—encrypting even 10 percent of an MPEG stream renders it effectively useless for illicit copying. On the other hand, the audio is entirely encrypted, and each audio block

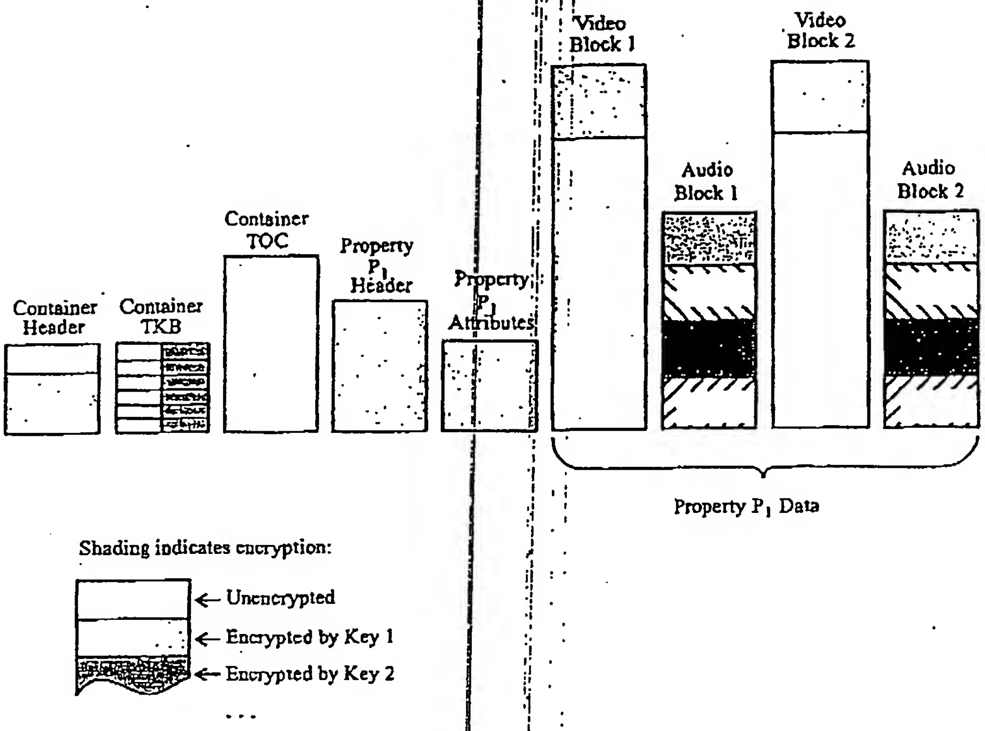

Figure 5. Container physical format.

uses four distinct keys, because the content proprietor requires much stronger security for audio than for video.

A property is represented as one or more property sections, each of which is independently associated with control information, and which may also be stored and accessed independently. A property, for example, might be a collection of clip-art images, and each image might be a property "chunk," with its own control specifying how that image's creator is compensated.

Controls can map to property chunks at arbitrary granularity and can enforce arbitrary organizational structures within the property (such as a file hierarchy). Controls can apply to individual bytes, frames of a movie, segments of a musical piece, and so on, because the mapping is performed by a control process specified by the control structure, not simply via a table-driven data structure.

5.3 Cryptographic Techniques

The high-level elements in a DigiBox are encrypted with a *transport key* that is normally derived (by exclusive OR) from two parts: one that is delivered in the DigiBox itself, encrypted with a public key algorithm, and the other that is stored in protected storage locally. The locally stored part is shared among all the local nodes capable of processing that DigiBox, but the part in the DigiBox is unique. This separation provides protection against accidental or malicious disclosure of either part.

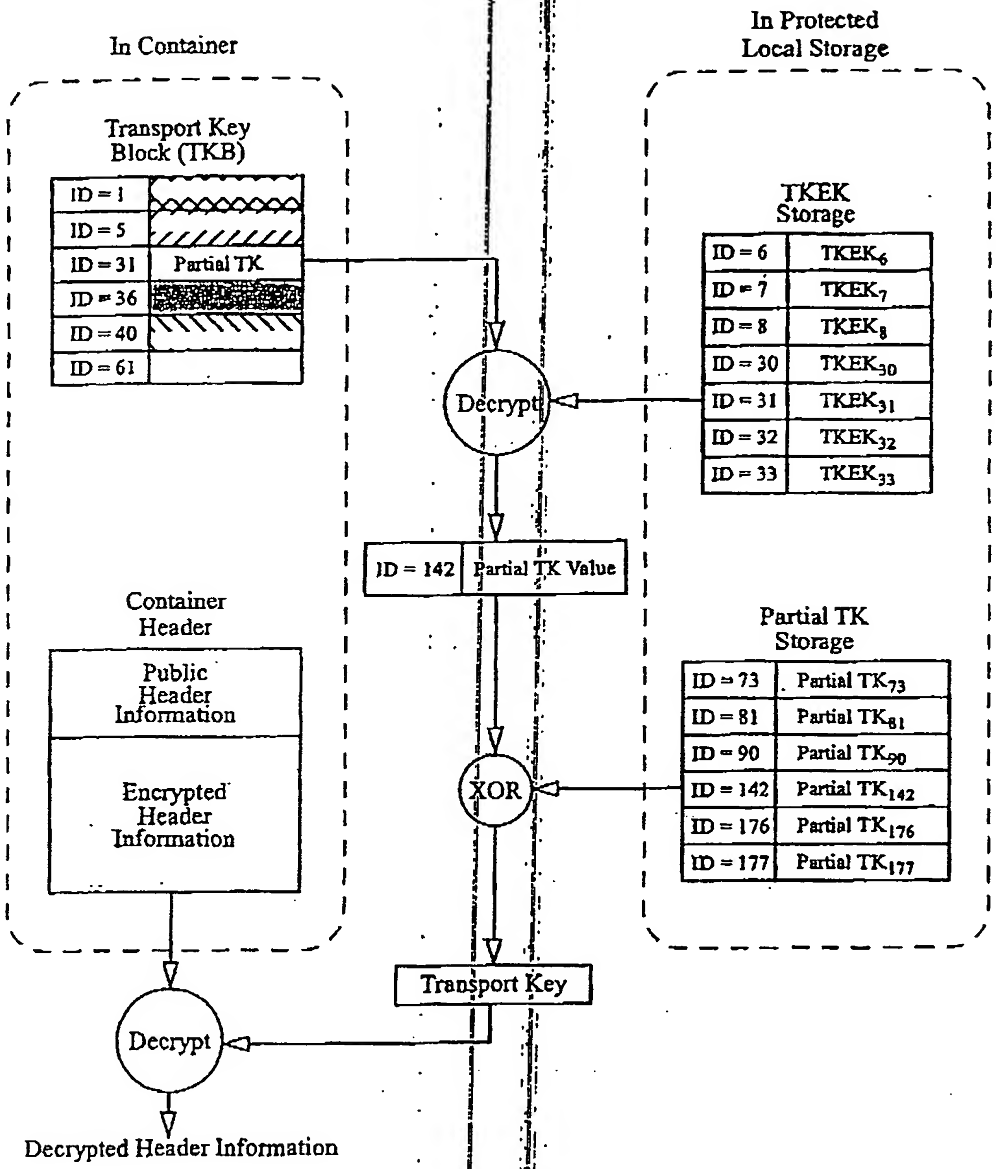

Figure 6. Container transport security.

Figure 6 illustrates how the transport key (TK) is derived. The transport key block (TKB) contains one or more slots, each of which contains a partial transport key encrypted under a different transport key encrypting key (TKEK). Each TKB slot identifies the TKEK used, and a matching TKEK is selected from local protected storage. Decrypting the slot yields a partial TK, which is combined with its corresponding partial TK again from protected local storage to yield the actual TK for decrypting the container header.

The data for the property itself is encrypted with other keys ("content keys") that are themselves delivered in encrypted high-level structures; this approach permits the keys for a property to be delivered entirely separately from the property or its controls. Multiple keys, in a wide variety of key-mapping schemes, are used to encrypt the data, limiting the loss that would occur from disclosure of any one key.

All DigiBox control structures are both encrypted and verified for integrity with a cryptographic hash function. Several cryptographic algorithms are supported for these control structures (principally for export control reasons), and arbitrary algorithms are supported for encryption of the data.

5.4 Security Characteristics

The DigiBox cryptographic structures are designed to be secure even in the face of loss of individual key components, and to minimize the damage in case a key or processing environment is compromised. The system is designed to provide commercially acceptable risks and losses for a variety of business models.

The basic algorithms are strong: Triple DES [22] and RSA [23] are preferred. This security is, of course, only as strong as the tamper-resistance of the local processing environment. The preferred implementation of DigiBox processing relies on a "secure processing unit" (SPU) that contains a CPU, memory, program storage, and key storage in a single tamper-resistant hardware package. Although these are not widely available today, the variety of applications they might support makes it likely that such SPUs will become widely integrated into common computing platforms. When running in an SPU, the DigiBox processing and control mechanisms are sufficiently well protected to support most commerce applications.

In the absence of an SPU, other approaches are useful for many business models. In fact, a software-only implementation is sufficient for many applications, because much content is of relatively low value and is used in a context (business to business) where a modest level of fraud is both less likely and more tolerable. As long as the software is moderately difficult to defeat and tools to defeat it have no legitimate purpose, business models can be supported where some risk of loss is acceptable. In the world of electronic commerce, just as for traditional commerce, security is not absolute: it is just a factor to balance against the cost of loss and fraud.

6 Conclusions

The DigiBox is one component of a general-purpose electronic commerce solution that rests on three basic principles: rights protection, interoperability, and strong security.

Electronic commerce, and information commerce in particular, needs a robust information protection mechanism, including rights protection and controls, not just payment systems. As the electronic world evolves, however, and moves forward from simply emulating traditional transactions into entirely new business models, rights protection and control will become the predominant issues.

Protection of intellectual property rights in information requires strong cryptography as well as a flexible infrastructure for controlling use of the information. A standard protected container for information is necessary to support interoperability—most existing schemes tightly bind the creator of protected information and the software that processes it. A standard container can rationalize information commerce and reduce costs for all participants.

In the long term, general-purpose secure electronic commerce will need pervasive deployment of tamper-resistant hardware devices to perform secure processing of protected content. However, as these solutions are developed, many business models can be accommodated with weaker or less complete solutions because the risk and expected losses are commercially acceptable.

Business-to-business purchasing is steadily evolving into a direct electronic ordering model. Future communications and media markets will become increasingly segmented and specialized in response to customer preferences and needs and involve increasing, and more sophisticated, direct interaction between consumers and providers. These markets and their value chains (with or without intermediary distributors) will require secure metering and control tools that enable a user to efficiently and economically tailor resources to his or her own desires.

During the next decade, digital delivery of traditional electronic products, such as information databases and software, will be joined by a rapidly growing array of both New Media and electronically distributed traditional content. The conversion from traditional models requires key foundation technologies and will result in a fundamental shift in current infrastructure. This transformation will create a new distribution industry. Digital distribution employing a universal content and commerce container can play a critical role in this broad economic transformation.

7 References

[1] A. Chandler and H. Daems, "Administrative Coordination, Allocation, and Monitoring: A Comparative Analysis of Accounting and Organization in the U.S.A. and Europe," *Accounting, Organizations and Society,* 1979: 3–20.

[2] O. Williamson, "The Modern Corporation: Origin, Evolution, Attributes," *Journal of Economic Literature* XIX (1981): 1537–1568.

[3] Office of Technology Assessment, *Accessibility and Integrity of Networked Information Collections.* Washington, D.C.: U.S. Government Printing Office, July, 1993.

[4] E. Hollings, *Communications Competitiveness and Infrastructure Modernization Act of 1990.* Washington, D.C.: U.S. Government Printing Office, report of the Senate Committee on Commerce, Science, and Transportation, 12 September 1990.

[5] R. Benjamin and R Wigand, "Electronic Markets and Virtual Value Chains on the Information Superhighway," *Sloan Management Review,* Vol. 36 No. 2 (1995).

[6] U.S. Constitution, Article 1, Section 8, Clause 8 (1787).

[7] U.S. Copyright Act of 1978

[8] 17 U.S.C. s107

[9] 17 U.S.C s102(a)

[10] T. Berners-Lee, R Caillian, and J.-F. Groff, "The World Wide Web," *Computer Networks and ISDN Systems,* Vol. 25 (Dec. 1992), pp 454–459.

[11] D. Chaum, "Achieving Electronic Privacy," *Scientific American,* August 1992, pp 96–101.

[12] M. Sirbu and J. D. Tygar, "NetBill: An Internet Commerce System," *IEEE CompCon Proceedings,* March, 1995, pp 20–25.

[13] D. Gifford et al., "Payment Switches for Open Networks," *IEEE CompCon Proceedings,* March, 1995, pp 26–31.

[14] S. Dukach, "SNPP: A Simple Network Payment Protocol," MIT Laboratory for Computer Science, Cambridge, MA, 1993.

[15] B. C. Neuman and G. Medvinsky., "Requirements for Network Payment," *IEEE CompCon Proceedings,* March, 1995, pp 32–36.

[16] First Virtual, Inc. "Introducing the First Virtual Internet Payment System," 1994.

[17] A. K. Choudhury, et al., "Copyright Protection for Electronic Publishing over Computer Networks," June 1994, *IEEE Network Magazine.*

[18] J. Erickson, "A Copyright Management System for Networked Interactive Multimedia," *Proceedings of the 1995 Dartmouth Institute for Advanced Graduate Studies,* 1995.

[19] K. Hickman, "SSL Reference Manual," Netscape Corporation World Wide Web Site, http://www.netscape.com/newsref/std/sslref.html, 1994.

[20] E. Rescorla and A. Schiffman, "The Secure HyperText Transfer Protocol," Internet Draft draft-resorla-shttp-0.txt, 1994.

[21] B. Cox, "Superdistribution," *Wired*, Sept. 1994, pp 89-92.

[22] U.S. National Bureau of Standards, "Data Encryption Standard," *Federal Information Processing Standards Publication*, FIPS PUB 46-1, Jan. 1988.

[23] R. Rivest, A. Shamir, and L. Adleman, "On Digital Signatures and Public-key Cryptosystems," *Communications of the ACM*, Vol. 21 (Feb. 1978), pp 120–126.

EXHIBIT B

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F	A2	(11) International Publication Number: WO 96/27155 (43) International Publication Date: 6 September 1996 (06.09.96)

(21) International Application Number: PCT/US96/02303

(22) International Filing Date: 13 February 1996 (13.02.96)

(30) Priority Data:
08/388,107 13 February 1995 (13.02.95) US

(71) Applicant: ELECTRONIC PUBLISHING RESOURCES, INC. [US/US]; 5203 Battery Lane, Bethesda, MD 20814 (US).

(72) Inventors: GINTER, Karl, L.; 10404 43rd Avenue, Beltsville, MD 20705 (US). SHEAR, Victor, H.; 5203 Battery Lane, Bethesda, MD 20814 (US). SPAHN, Francis, J.; 2410 Edwards Avenue, El Cerrito, CA 94530 (US). VAN WIE, David, M.; 1250 Lakeside Drive, Sunnyvale, CA 94086 (US).

(74) Agent: FARIS, Robert, W.; Nixon & Vanderhye P.C., 1100 North Glebe Road, Arlington, VA 22201-4714 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AZ, BY, KG, KZ, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION

(57) Abstract

The present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Secure distributed and other operating system environments and architectures, employing, for example, secure semiconductor processing arrangements that may establish secure, protected environments at each node. These techniques may be used to support an end-to-end electronic information distribution capability that may be used, for example, utilizing the "electronic highway".

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
CHRISTOPHER P. ISAAC
1300 I Street, N.W.
Washington, D.C. 20005-3314
Telephone: (202) 408-4000
Facsimile: (202) 408-4400

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01 1640 SBA **THIRD AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 6,185,683 B1; 6,253,193 B1; 5,940, 504; 5,920,861; 5,892,900; 5,982,891; AND 5,917,912.** **DEMAND FOR JURY TRIAL**

Plaintiff INTERTRUST TECHNOLOGIES CORPORATION (hereafter "InterTrust") hereby complains of Defendant MICROSOFT CORPORATION (hereafter "Microsoft"), and alleges as follows:

JURISDICTION AND VENUE

1. This action for patent infringement arises under the patent laws of the United States,

Title 35, United States Code, more particularly 35 U.S.C. §§ 271 and 281.

2. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(c) and 1400(b).

THE PARTIES

4. Plaintiff InterTrust is a Delaware corporation with its principal place of business at 4750 Patrick Henry Drive, Santa Clara, California.

5. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft is a Washington Corporation with its principal place of business at One Microsoft Way, Redmond, Washington.

6. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft does business in this judicial district and has committed and is continuing to commit acts of infringement in this judicial district.

7. InterTrust is the owner of United States Patent No. 6,185,683 B1, entitled "Trusted and secure techniques, systems and methods for item delivery and execution" ("the '683 patent"), duly and lawfully issued on February 6, 2001.

8. InterTrust is the owner of United States Patent No. 6,253,193 B1, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '193 patent"), duly and lawfully issued on June 26, 2001.

9. InterTrust is the owner of United States Patent No. 5,940,504, entitled "Licensing management system and method in which datagrams including an address of a licensee and indicative of use of a licensed product are sent from the licensee's site" ("the '504 patent"), duly and lawfully issued on August 17, 1999.

10. InterTrust is the owner of United States Patent No. 5,920,861, entitled "Techniques for defining, using and manipulating rights management data structures" ("the '861 patent"), duly and lawfully issued on July 6, 1999.

11. InterTrust is the owner of United States Patent No. 5,892,900, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '900 patent"), duly and lawfully issued on April 6, 1999.

12. InterTrust is the owner of United States Patent No. 5,982,891, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '891 patent"), duly and lawfully issued on November 9, 1999.

13. InterTrust is the owner of United States Patent No. 5,917,912 entitled "System and methods for secure transaction management and electronic rights protection" ("the '912 patent"), duly and lawfully issued on June 29, 1999.

FIRST CLAIM FOR RELIEF

14. InterTrust hereby incorporates by reference paragraphs 1-7 as if restated herein.

15. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

16. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '683 patent under § 271(a) by making and using systems incorporating Windows Media Player Versions 7 and 8. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '683 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(a) will continue unless enjoined by this Court.

17. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '683 patent under § 271(a), thereby inducing infringement of the '683 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(b) will continue unless enjoined by this Court.

18. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '683 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing

use, including at least Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under §271(c) will continue unless enjoined by this Court.

19. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '683 patent in the manner described above in paragraphs 16 through 18, and will continue to do so unless enjoined by this Court.

20. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SECOND CLAIM FOR RELIEF

21. InterTrust hereby incorporates by reference paragraphs 1-6 and 8 as if restated herein.

22. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

23. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '193 patent under § 271(a) by using Windows Media Player Versions 7 and 8. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '193 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(a) will continue unless enjoined by this Court.

24. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '193 patent under § 271(a), thereby inducing infringement of the '193 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's

infringement of the '193 patent under §271(b) will continue unless enjoined by this Court.

25. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '193 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least Windows Media Player Versions 7 and 8. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under §271(c) will continue unless enjoined by this Court.

26. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '193 patent in the manner described above in paragraphs 23 through 25, and will continue to do so unless enjoined by this Court.

27. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

THIRD CLAIM FOR RELIEF

28. InterTrust hereby incorporates by reference paragraphs 1-6 and 9 as if restated herein.

29. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

30. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '504 patent under § 271(a) by Microsoft's use of the Product Activation feature of Windows XP, Office XP, and other Microsoft products. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '504 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '504 patent under §271(a) will continue unless enjoined by this Court.

31. InterTrust is informed and believes, and on that basis alleges, that Microsoft has

been and is knowingly and intentionally inducing others to infringe directly the '504 patent under § 271(a), thereby inducing infringement of the '504 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of the Product Activation feature of Windows XP, Office XP, and other Microsoft products. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '504 patent under §271(b) will continue unless enjoined by this Court.

32. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '504 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including the Product Activation feature of Windows XP, Office XP, and other Microsoft products. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '504 patent under §271(c) will continue unless enjoined by this Court.

33. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '504 patent in the manner described above in paragraphs 30 through 32, and will continue to do so unless enjoined by this Court.

34. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

FOURTH CLAIM FOR RELIEF

35. InterTrust hereby incorporates by reference paragraphs 1-6 and 10 as if restated herein.

36. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

37. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '861 patent under § 271(a) by making, using, selling, and offering for

sale digital rights management software incorporating inventions claimed in the '861 patent, including but not limited to the Digital Asset Server and Microsoft Reader. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, including Microsoft's .NET architecture, which infringe the '861 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under §271(a) will continue unless enjoined by this Court.

38. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '861 patent under § 271(a), thereby inducing infringement of the '861 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of Digital Asset Server, Microsoft Reader, and the .NET architecture. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under §271(b) will continue unless enjoined by this Court.

39. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '861 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including but not limited to the Digital Asset Server and Microsoft Reader. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under §271(c) will continue unless enjoined by this Court.

40. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '861 patent in the manner described above in paragraphs 37 through 39, and will continue to do so unless enjoined by this Court.

41. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

FIFTH CLAIM FOR RELIEF

42. InterTrust hereby incorporates by reference paragraphs 1-6 and 11 as if restated herein.

43. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

44. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '900 patent under § 271(a) by Microsoft's use of the Product Activation feature of Windows XP, Office XP, and other Microsoft products. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '900 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '900 patent under §271(a) will continue unless enjoined by this Court.

45. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '900 patent under § 271(a), thereby inducing infringement of the '900 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of the Product Activation feature of Windows XP, Office XP, and other Microsoft products. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '900 patent under §271(b) will continue unless enjoined by this Court.

46. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '900 patent under § 271(c) by providing digital rights management software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including the Product Activation feature of Windows XP, Office XP, and other Microsoft products. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '900 patent under §271(c) will continue unless enjoined by this Court.

47. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '900 patent in the manner described above in paragraphs 44 through 46, and will continue to do so unless enjoined by this Court.

48. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SIXTH CLAIM FOR RELIEF

49. InterTrust hereby incorporates by reference paragraphs 1-6 and 12 as if restated herein.

50. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

51. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '891 patent under § 271(a) by Microsoft's implementation of its .NET architecture. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '891 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under §271(a) will continue unless enjoined by this Court.

52. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '891 patent under § 271(a), thereby inducing infringement of the '891 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its .NET architecture. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under §271(b) will continue unless enjoined by this Court.

53. InterTrust is informed and believes, and on that basis alleges, that Microsoft has

been and is contributorily infringing the '891 patent under § 271(c) by providing .NET software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under §271(c) will continue unless enjoined by this Court.

54. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '891 patent in the manner described above in paragraphs 51 through 53, and will continue to do so unless enjoined by this Court.

55. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SEVENTH CLAIM FOR RELIEF

56. InterTrust hereby incorporates by reference paragraphs 1-6 and 13 as if restated herein.

57. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

58. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '912 patent under § 271(a) by Microsoft's implementation of its .NET architecture. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '912 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '912 patent under §271(a) will continue unless enjoined by this Court.

59. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '912 patent under § 271(a), thereby inducing infringement of the '912 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which

Microsoft has promoted and marketed use of its .NET architecture. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '912 patent under §271(b) will continue unless enjoined by this Court.

60. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '912 patent under § 271(c) by providing .NET software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '912 patent under §271(c) will continue unless enjoined by this Court.

61. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '912 patent in the manner described above in paragraphs 58 through 60, and will continue to do so unless enjoined by this Court.

62. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, InterTrust prays for relief as follows:

A. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(a);

B. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '683 patent under 35 U.S.C. § 271(a);

C. That Microsoft be adjudged to have contributorily infringed the '683 patent under 35 U.S.C. § 271(c);

D. That Microsoft be adjudged to have willfully infringed the '683 patent under 35 U.S.C. §§ 271(a), (b), and (c);

E. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '683 patent;

F. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(a);

G. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '193 patent under 35 U.S.C. § 271(a);

H. That Microsoft be adjudged to have contributorily infringed the '193 patent under 35 U.S.C. § 271(c);

I. That Microsoft be adjudged to have willfully infringed the '193 patent under 35 U.S.C. §§ 271(a), (b), and (c);

J. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '193 patent;

K. That Microsoft be adjudged to have infringed the '504 patent under 35 U.S.C. § 271(a);

L. That Microsoft be adjudged to have infringed the '504 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '504 patent under 35 U.S.C. § 271(a);

M. That Microsoft be adjudged to have contributorily infringed the '504 patent under 35 U.S.C. § 271(c);

N. That Microsoft be adjudged to have willfully infringed the '504 patent under 35 U.S.C. §§ 271(a), (b), and (c);

O. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '504 patent;

P. That this Court award damages to compensate InterTrust for Microsoft's infringement, as well as enhanced damages, pursuant to 35 U.S.C. § 284;

Q. That this Court adjudge this case to be exceptional and award reasonable attorney's fees to InterTrust pursuant to 35 U.S.C. § 285;

R. That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. § 271(a);

S. That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '861 patent under 35 U.S.C. § 271(a);

T. That Microsoft be adjudged to have contributorily infringed the '861 patent under 35 U.S.C. § 271(c);

U. That Microsoft be adjudged to have willfully infringed the '861 patent under 35 U.S.C. §§ 271(a), (b), and (c);

V. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '861 patent;

W. That Microsoft be adjudged to have infringed the '900 patent under 35 U.S.C. § 271(a);

X. That Microsoft be adjudged to have infringed the '900 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '900 patent under 35 U.S.C. § 271(a);

Y. That Microsoft be adjudged to have contributorily infringed the '900 patent under 35 U.S.C. § 271(c);

Z. That Microsoft be adjudged to have willfully infringed the '900 patent under 35 U.S.C. §§ 271(a), (b), and (c);

AA. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '900 patent;

BB. That Microsoft be adjudged to have infringed the '891 patent under 35 U.S.C. § 271(a);

CC. That Microsoft be adjudged to have infringed the '891 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '891 patent under 35 U.S.C. § 271(a);

DD. That Microsoft be adjudged to have contributorily infringed the '891 patent under

35 U.S.C. § 271(c);

EE. That Microsoft be adjudged to have willfully infringed the '891 patent under 35 U.S.C. §§ 271(a), (b), and (c);

FF. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '891 patent;

GG. That Microsoft be adjudged to have infringed the '912 patent under 35 U.S.C. § 271(a);

HH. That Microsoft be adjudged to have infringed the '912 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '912 patent under 35 U.S.C. § 271(a);

II. That Microsoft be adjudged to have contributorily infringed the '912 patent under 35 U.S.C. § 271(c);

JJ. That Microsoft be adjudged to have willfully infringed the '912 patent under 35 U.S.C. §§ 271(a), (b), and (c);

KK. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '912 patent;

LL. That this Court assess pre-judgment and post-judgment interest and costs against Microsoft, and award such interest and costs to InterTrust, pursuant to 35 U.S.C. § 284; and

MM. That InterTrust have such other and further relief as the Court may deem proper.

Dated: October 26, 2001

KEKER & VAN NEST, LLP

By:______________________________
MICHAEL H. PAGE
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

DEMAND FOR JURY TRIAL

Plaintiff InterTrust herby demands a trial by jury as to all issues triable by jury, specifically including, but not limited to, the issue of infringement of United States Patent Nos. 6,185,683 B1; 6,253,193 B1; 5,940,504; 5,920,861; 5,892,900; 5,982,891; and 5,917,912.

Dated: October 26, 2001

KEKER & VAN NEST, LLP

By: ____________________
MICHAEL H. PAGE
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	CASE NO. C01-1640 SBA **MICROSOFT CORPORATION'S ANSWER AND COUNTERCLAIMS TO INTERTRUST'S THIRD AMENDED COMPLAINT; JURY DEMAND**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	

Defendant Microsoft Corporation ("Microsoft") answers the Third Amended Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

1. Microsoft admits that the Third Amended Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Third Amended Complaint.

2. Microsoft admits that the Third Amended Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Third Amended Complaint.

4. On information and belief, Microsoft admits the allegations of paragraph 4 of the Third Amended Complaint.

5. Microsoft admits the allegations of paragraph 5 of the Third Amended Complaint.

6. Microsoft admits, for purposes of this action only, that it transacts business in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the Third Amended Complaint.

7. Microsoft admits that on its face the title page of U.S. Patent No. 6,185,683 B1 ("the '683 Patent") states that it was issued February 6, 2001, is entitled "Trusted and secure techniques, systems and methods for item delivery and execution," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '683 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 7 of the Third Amended Complaint.

8. Microsoft admits that on its face the title page of U.S. Patent No. 6,253,193 B1 ("the '193 Patent") states that it was issued June 26, 2001, is entitled "Systems and methods for the secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corporation" as the assignee.. Microsoft denies that the '193 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 8 of the Third Amended Complaint.

9. Microsoft admits that on its face the title page of U.S. Patent No. 5,940,504 ("the '504 Patent") states that it was issued August 17, 1999, and is entitled "Licensing management system and method in which datagrams including an address of a licensee and indicative of use of a licensed product are sent from the licensee's site." Microsoft denies that the '504 Patent was duly and lawfully issued. Microsoft lacks sufficient information to admit or deny any and all remaining allegations of paragraph 9 of the Third Amended Complaint.

10. Microsoft admits that on its face the title page of U.S. Patent No. 5,920,861 ("the '861 Patent") states that it was issued July 6, 1999, is entitled "Techniques for defining using and manipulating rights management data structures," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '861 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 10 of the Third Amended Complaint.

11. Microsoft admits that on its face the title page of U.S. Patent No. 5,892,900 ("the '900 Patent") states that it was issued April 6, 1999, is entitled "Systems and methods for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '900 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 11 of the Third Amended Complaint.

12. Microsoft admits that on its face the title page of U.S. Patent No. 5,982,891 ("the '891 Patent") states that it was issued November 9, 1999, is entitled "Systems and methods for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '891 Patent was duly and lawfully

issued. Microsoft further denies any and all remaining allegations of paragraph 12 of the Third Amended Complaint.

13. Microsoft admits that on its face the title page of U.S. Patent No. 5,917,912 ("the '912 Patent") states that it was issued June 29, 1999, is entitled "System and methods for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '912 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 13 of the Third Amended Complaint.

14. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Third Amended Complaint, as if fully restated herein.

15. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 15 of the Third Amended Complaint.

16. Microsoft denies any and all allegations of paragraph 16 of the Third Amended Complaint.

17. Microsoft denies any and all allegations of paragraph 17 of the Third Amended Complaint.

18. Microsoft denies any and all allegations of paragraph 18 of the Third Amended Complaint.

19. Microsoft denies any and all allegations of paragraph 19 of the Third Amended Complaint.

20. Microsoft denies any and all allegations of paragraph 20 of the Third Amended Complaint.

21. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 8 of the Third Amended Complaint, as if fully restated herein.

22. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now

infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 22 of the Third Amended Complaint.

23. Microsoft denies any and all allegations of paragraph 23 of the Third Amended Complaint.

24. Microsoft denies any and all allegations of paragraph 24 of the Third Amended Complaint.

25. Microsoft denies any and all allegations of paragraph 25 of the Third Amended Complaint.

26. Microsoft denies any and all allegations of paragraph 26 of the Third Amended Complaint.

27. Microsoft denies any and all allegations of paragraph 27 of the Third Amended Complaint.

28. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 9 of the Third Amended Complaint, as if fully restated herein.

29. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 29 of the Third Amended Complaint.

30. Microsoft denies any and all allegations of paragraph 30 of the Third Amended Complaint.

31. Microsoft denies any and all allegations of paragraph 31 of the Third Amended Complaint.

32. Microsoft denies any and all allegations of paragraph 32 of the Third Amended Complaint.

33. Microsoft denies any and all allegations of paragraph 33 of the Third Amended Complaint.

34. Microsoft denies any and all allegations of paragraph 34 of the Third Amended Complaint.

35. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 10 of the Third Amended Complaint, as if fully restated herein.

36. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 36 of the Third Amended Complaint.

37. Microsoft denies any and all allegations of paragraph 37 of the Third Amended Complaint.

38. Microsoft denies any and all allegations of paragraph 38 of the Third Amended Complaint.

39. Microsoft denies any and all allegations of paragraph 39 of the Third Amended Complaint.

40. Microsoft denies any and all allegations of paragraph 40 of the Third Amended Complaint.

41. Microsoft denies any and all allegations of paragraph 41 of the Third Amended Complaint.

42. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 11 of the Third Amended Complaint, as if fully restated herein.

43. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 43 of the Third Amended Complaint.

44. Microsoft denies any and all allegations of paragraph 44 of the Third Amended Complaint.

45. Microsoft denies any and all allegations of paragraph 45 of the Third Amended Complaint.

46. Microsoft denies any and all allegations of paragraph 46 of the Third Amended Complaint.

47. Microsoft denies any and all allegations of paragraph 47 of the Third Amended Complaint.

·48. Microsoft denies any and all allegations of paragraph 48 of the Third Amended Complaint.

49. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 12 of the Third Amended Complaint, as if fully restated herein.

50. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 50 of the Third Amended Complaint.

51. Microsoft denies any and all allegations of paragraph 51 of the Third Amended Complaint.

52. Microsoft denies any and all allegations of paragraph 52 of the Third Amended Complaint.

53. Microsoft denies any and all allegations of paragraph 53 of the Third Amended Complaint.

54. Microsoft denies any and all allegations of paragraph 54 of the Third Amended Complaint.

55. Microsoft denies any and all allegations of paragraph 55 of the Third Amended Complaint.

56. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 13 of the Third Amended Complaint, as if fully restated herein.

57. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 57 of the Third Amended Complaint.

58. Microsoft denies any and all allegations of paragraph 58 of the Third Amended Complaint.

59. Microsoft denies any and all allegations of paragraph 59 of the Third Amended Complaint.

60. Microsoft denies any and all allegations of paragraph 60 of the Third Amended Complaint.

61. Microsoft denies any and all allegations of paragraph 61 of the Third Amended Complaint.

62. Microsoft denies any and all allegations of paragraph 62 of the Third Amended Complaint.

AFFIRMATIVE AND OTHER DEFENSES

Further answering the Third Amended Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patents

63.. Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,185,683 B1 ("the '683 Patent"), U.S. Patent No. 6,253,193 B1 ("the '193 Patent"), U.S. Patent No. 5,940,504 ("the '504 Patent"), U.S. Patent No. 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), or U.S. Patent No. 5,917,912 ("the '912 Patent"), and is not liable for infringement thereof.

64. Any and all Microsoft products or methods that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent.

Second Defense: Invalidity of the Asserted Patents

65. On information and belief, the '683 Patent, the '193 Patent, the '504 Patent the '861 Patent, the '900 Patent, the '891 Patent, and the '912 Patent are invalid for failing to comply with the provisions of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailability of Relief

66. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 271(b) and (c) and is not entitled to any alleged damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent.

Fourth Defense: Unavailability of Relief

67. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent and any alleged infringement thereof.

Fifth Defense: Unavailability of Relief

68. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any damages.

Sixth Defense: Prosecution History Estoppel

69. Plaintiff's alleged causes of action for patent infringement are barred under the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

70. Plaintiff has dedicated to the public all methods, apparatus, and products disclosed in the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent, but not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture By/For United States Government

71. To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

72. To the extent that any of Plaintiff's allegations of infringement are premised on the alleged use, sale, offer for sale, license or offer of license of products that were manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft by or to a licensee of InterTrust, such allegations are barred pursuant to license.

Tenth Defense: Acquiescence

73. Plaintiff has acquiesced in at least a substantial part of the Microsoft conduct alleged to infringe.

Eleventh Defense: Laches

74. Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

75. The '861 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '861 Patent, set forth below.

Thirteenth Defense: Inequitable Conduct

76. The '900 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '900 Patent, set forth below.

Fourteenth Defense: Unenforceability

77. The claims of the '891 Patent, the '912 Patent, the '861 Patent, the '683 Patent, the '193 Patent and the '900 Patent are unenforceable due to unclean hands, inequitable conduct and misuse and illegal extension of the patent right, including those acts and failures to act set forth in Count XI of Microsoft's Counterclaims, set forth below.

///

///

///

///

COUNTERCLAIMS

COUNT I - DECLARATORY JUDGMENT OF NONINFRINGEMENT

78. This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, *et seq.* This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

79. Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

80. On information and belief, Plaintiff /Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

81. InterTrust purports to be the owner of U.S. Patent Nos. 6,185,683 B1 ("the '683 Patent"), 6,253,193 B1 ("the '193 Patent"), 5,940,504 ("the '504 Patent"), 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), and U.S. Patent No. 5,917,912 ("the '912 Patent").

82. InterTrust alleges that Microsoft has infringed the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and the '912 Patent.

83. No Microsoft product has infringed, either directly or indirectly, any claim of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent, and Microsoft is not liable for infringement thereof.

84. An ~~actual controversy, within the meaning of~~ 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the infringement or noninfringement of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent.

COUNT II - DECLARATORY JUDGMENT OF INVALIDITY OF THE '683 PATENT

85. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

86. The '683 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

87. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '683 Patent are valid or invalid.

COUNT III - DECLARATORY JUDGMENT
OF INVALIDITY OF THE '193 PATENT

88. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

89. The '193 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

90. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '193 Patent are valid or invalid.

COUNT IV - DECLARATORY JUDGMENT
OF INVALIDITY OF THE '504 PATENT

91. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

92. The '504 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

93. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '504 Patent are valid or invalid.

COUNT V - DECLARATORY JUDGMENT
OF INVALIDITY OF THE '861 PATENT

94. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

95. The '861 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

96. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are valid or invalid.

COUNT VI - DECLARATORY JUDGMENT OF INVALIDITY OF THE '900 PATENT

97. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

98. The '900 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

99. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are valid or invalid.

COUNT VII - DECLARATORY JUDGMENT OF INVALIDITY OF THE '891 PATENT

100. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

101. The '891 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

102. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '891 Patent are valid or invalid.

COUNT VIII - DECLARATORY JUDGMENT OF INVALIDITY OF THE '912 PATENT

103. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

104. The '912 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

105. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '912 Patent are valid or invalid.

COUNT IX - DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '861 PATENT

106. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

107. Claims 1-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, were not and are not entitled to the benefit of any application filing date prior to February 25, 1997, under 35 U.S.C. § 120 or otherwise.

108. "Exhibit A" refers to the document attached as Exhibit A to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a reprint of an article entitled "DigiBox: A Self-Protecting Container for Information Commerce").

109. On information and belief, the content of pages 2-14 of Exhibit A was presented at a public conference in the United States in July 1995.

110. "Exhibit B" refers to the document attached as Exhibit B to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a copy of a page from an International Application published under the Patent Cooperation Treaty (PCT), bearing International Publication Number WO-96/27155).

111. On information and belief, International Application WO 96/27155 has, at all times since its filing date, been owned and controlled by InterTrust or its predecessors in interest.

112. International Application WO 96/27155 (hereafter "the WO 96/27155 (PCT) publication") was published on September 6, 1996.

113. United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8, 1999, from a continuation of an application filed on February 13, 1995.

114. The Sibert article is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

115. The Sibert article is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. §§ 102(b).

116. The WO 96/27155 (PCT) publication is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

117. The WO 96/27155 (PCT) publication is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. §§ 102(a).

118. The '987 Patent is prior art to claims 29-129 of the '861 Patent application (SN 08/805,804).

119. The '987 Patent is prior art to claims 1-101 of the '861 Patent, under 35 U.S.C. §§ 102(e).

120. The Sibert article was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

121. The Sibert article was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

122. The WO 96/27155 (PCT) publication was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

123. The WO 96/27155 (PCT) publication was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

124. The '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804).

125. One or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the July 1995 publication of the Sibert article.

126. On information and belief, one or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

127. One or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the June 8, 1999 issuance of the '987 Patent.

128. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the July 1995 publication of the Sibert article.

129. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

130. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the June 8, 1999 issuance of the '987 Patent.

131. The applicants for the '861 Patent did not cite the Sibert article as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

132. The applicants for the '861 Patent did not cite the WO 96/27155 (PCT) publication to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

133. The applicants for the '861 Patent did not cite the '987 Patent to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

134. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the Sibert article.

135. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the WO 96/27155 (PCT) publication.

136. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the '987 Patent.

137. The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

138. The WO 96/27155 (PCT) publication is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

139. The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

140. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

141. InterTrust contends that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article discloses an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

142. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

143. It is InterTrust's contention that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication discloses an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

144. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the Sibert article was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

145. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the WO 96/27155 (PCT) publication was material to the patentability of claims 1-129 of the '861 Patent application

(SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

146. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

147. The '861 Patent is unenforceable due to the inequitable conduct of the '861 Patent applicants before the Patent and Trademark Office in connection with the '861 Patent application (SN 08/805,804).

148. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are enforceable.

COUNT X - DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '900 PATENT

149. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

150. The application and issued claims of the '900 Patent were not and are not entitled to the benefit of any application filing date prior to August 30, 1996, under 35 U.S.C. § 120 or otherwise.

151. Microsoft repeats and realleges paragraphs 31-32 of its Counterclaims, as if fully restated herein.

152. The Sibert article is prior art to the application and issued claims of the '900 Patent under 35 U.S.C. § 102(a), 103.

153. The Sibert article was material to the patentability of application and issued claims of the '900 Patent, including, for example, issued claims 86 and 182.

154. One or more of the '900 Patent applicants knew of the July 1995 publication of the Sibert article while the '900 Patent application was pending.

155. On information and belief, one or more of the attorneys who prosecuted or assisted in the prosecution of the ‘900 Patent application knew of the July 1995 publication of the Sibert article while the ‘900 Patent application was pending.

156. The applicants for the ‘900 Patent did not cite the Sibert article to the Patent Office as prior art to any claims of the ‘900 Patent application (SN 08/706,206).

157. The applicants for the ‘900 Patent did not cite to the Patent Office as prior art to any claims of the ‘900 Patent application (SN 08/706,206) any reference having the same or substantially the same disclosure as the Sibert article.

158. The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the ‘900 Patent application (SN 08/706,206).

159. On information and belief, one or more of the ‘900 Patent applicants believed, during pendency of claim 1 of the ‘900 Patent application (SN 08/706,206), that the Sibert article disclosed an embodiment of claim 1 of the ‘900 Patent application (SN 08/706,206).

160. On information and belief, one or more of the ‘900 Patent applicants believed, while the ‘900 Patent application (SN 08/706,206) was pending, that the Sibert article was material to the patentability of various claims of the ‘900 Patent application (SN 08/706,206), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

161. International Application WO 96/27155 (hereafter "the WO 96/27155 (PCT) publication") was published on September 6, 1996.

162. The WO 96/27155 (PCT) publication is prior art to the application and issued claims of the ’900 Patent.

163. The WO 96/27155 (PCT) publication was material to the patentability of various application and issued claims of the ’900 Patent, including issued claims 86 and 182.

164. On information and belief, one or more of the ‘900 Patent applicants knew, while the ‘900 Patent application (SN 08/706,206) was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

165. One or more of the attorneys who prosecuted or assisted in prosecuting the '900 Patent application (SN 08/706,206) knew, while that application was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

166. The applicants for the '900 Patent did not cite the WO 96/27155 (PCT) publication to the Patent Office as prior art to any claims of '900 Patent application (SN 08/706,206).

167. The applicants for the '900 Patent did not cite to the Patent Office as prior art to any claims of the '900 Patent application (SN 08/706,206) any reference having the same or substantially the same disclosure as the WO 96/27155 (PCT) publication.

168. The WO 96/27155 (PCT) publication is not merely cumulative over any reference cited as prior art during the prosecution of the '900 Patent application (SN 08/706,206).

169. On information and belief, one or more of the '900 Patent applicants believed, while the '900 Patent application (SN 08/706,206) was pending, that the WO 96/27155 (PCT) publication was material to the patentability of various claims of the '900 Patent application (SN 08/706,206), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

170. The '900 Patent is unenforceable due to the inequitable conduct of the '900 Patent applicants before the Patent and Trademark Office in connection with the '900 Patent application (SN 08/706,206).

171. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are enforceable.

COUNT XI - DECLARATORY JUDGMENT OF UNENFORCEABILITY

172. Microsoft repeats and realleges paragraphs 1-5 and 30-94 of its Counterclaims, as if fully restated herein.

173. The '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent, and the '900 Patent are referred to as the Count XI Patents.

174. In prosecuting, marketing, and enforcing the Count XI Patents, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents. For example, InterTrust has accused non-infringing products of infringement, has buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the particular claims in issue, and has buried the Examiners with hundreds or thousands of pages of redundant, verbose, unclear text, effectively prohibiting a real comparison of the alleged "invention" versus the prior art. This pattern of intentional conduct constitutes an abuse of the patent system, unclean hands, misuse and illegal extension of the patent right, rendering the Count XI patents unenforceable, as well as invalid under Section 112.

175. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent, and the '900 Patent are enforceable.

COUNT XII - INFRINGEMENT OF U.S. PATENT NO. 6,049,671

176. Microsoft repeats and realleges paragraphs 2-3 of its Counterclaims, as if fully restated herein.

177. This Court has exclusive subject matter jurisdiction over Microsoft's cause of action for patent infringement under Title 28, United States Code, Sections 1331 and 1338, and under the patent laws of the United States, Title 35 of the United States Code.

178. U.S. Patent No. 6,049,671 ("the '671 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on April 11, 2000.

179. A true copy of the '671 Patent is attached as Exhibit C to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

180. Microsoft owns all right, title and interest in the '671 Patent.

181. InterTrust has had actual notice of the '671 Patent.

182. InterTrust has infringed one or more claims of the '671 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

183. InterTrust's infringement of the '671 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

COUNT XIII - INFRINGEMENT OF U.S. PATENT NO. 6,256,668

184. Microsoft repeats and realleges paragraphs 2-3 and 100 of its Counterclaims, as if fully restated herein.

185. U.S. Patent No. 6,256,668 B1 ("the '668 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on July 3, 2001.

186. A true copy of the '668 Patent is attached as Exhibit D to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

187. Microsoft owns all right, title and interest in the '668 Patent.

188. InterTrust has had actual notice of the '668 Patent.

189. InterTrust has infringed one or more claims of the '668 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

190. InterTrust's infringement of the '668 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A. The Court enter judgment against InterTrust, and dismiss with prejudice, any and all claims of the Third Amended Complaint;

B. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '683 Patent;

C. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '193 Patent;

D. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '504 Patent;

E. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '861 Patent;

F. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '900 Patent;

G. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '891 Patent;

H. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '912 Patent;

I. The Court enter judgment declaring that the '683 Patent is invalid;

J. The Court enter judgment declaring that the '193 Patent is invalid;

K. The Court enter judgment declaring that the '504 Patent is invalid;

L. The Court enter judgment declaring that the '861 Patent is invalid;

M. The Court enter judgment declaring that the '900 Patent is invalid;

N. The Court enter judgment declaring that the '891 Patent is invalid;

O. The Court enter judgment declaring that the '912 Patent is invalid;

P. The Court enter judgment declaring that the '861 Patent is unenforceable due to inequitable conduct;

Q. The Court enter judgment declaring that the '900 Patent is unenforceable due to inequitable conduct;

R. The Court enter judgment declaring that the '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent and the '900 Patent is unenforceable due to an abuse of the patent system, unclean hands, and misuse and illegal extension of the patent right;

S. The Court enter judgment that InterTrust has infringed the '671 Patent;

T. The Court enter judgment that InterTrust has infringed the '668 Patent;

U. The Court enter a permanent injunction prohibiting InterTrust, its officers, agents, servants; employees, and all persons in active concert or participation with any of them from infringing the '671 and '668 Patents;

V. The Court award damages and attorney fees against InterTrust pursuant to the provisions of 35 U.S.C §§ 284 and 285;

W. The Court award to Microsoft pre-judgment interest and the costs of this action;

X. The Court award to Microsoft its reasonable costs and attorneys' fees; and

Y. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

DATED: November 8, 2001

By:
WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Attorneys for Defendant
Microsoft Corporation

Of Counsel:

T. ANDREW CULBERT, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

DECLARATION OF SERVICE VIA ELECTRONIC MAIL AND U.S. MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 1000 Marsh Road, Menlo Park, California 94025.

On November 8, 2001, I served:

MICROSOFT CORPORATION'S ANSWER AND COUNTERCLAIMS TO INTERTRUST'S THIRD AMENDED COMPLAINT; JURY DEMAND

By transmitting a copy of the above-listed document(s) in PDF form via electronic mail **Michael H. Page at mhp@kvn.com, Christopher P. Isaac at chris.isaac@finnegan.com** and **James E. Geringer** at **james.geringer@klarquist.com** and also by placing true and correct copies of the above documents in an envelope addressed to:

John W. Keker, Esq.
Michael H. Page, Esq.
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111
Tel. No. 415-391-5400
Fax No. 415-397-7188
Email: jwk@kvn.com
Email: mhp@kvn.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Stephen E. Taylor, Esq. **(Served by U.S. Mail Only)**
TAYLOR & CO. LAW OFFICES
1050 Marina Village Parkway, Suite 101
Alameda, CA 94501
Tel. No. 510-865-9401
Fax No. 510-865-9408

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Christopher P. Isaac, Esq.
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER LLP
1300 I. Street, N.W.
Washington, DC 20005-3314
Tel. No. 202-408-4000
Fax No. 202-408-4400
Email: chris.isaac@finnegan.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

John D. Vandenberg, Esq.
James E. Geringer, Esq.
KLARQUIST, SPARKMAN, CAMPBELL,
LEIGH & WHINSTON LLP
One World Trade Center
121 S. W. Salmon Street, Suite 1600
Portland, Oregon 97204
Tel. No: 503-226-7391
Fax No: 503-228-9446
Email: john.vandenberg@klarquist.com
Email: james.geringer@klarquist.com

Attorneys for Defendant and
Counterclaimant, MICROSOFT
CORPORATION

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Menlo Park, California.

Executed on November 8, 2001 at Menlo Park, California.

I declare under penalty of perjury that the foregoing is true and correct.

____
(SIGNATURE)

____
(PRINT NAME)

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	CASE NO. C01-1640 SBA **MICROSOFT CORPORATION'S AMENDED ANSWER AND COUNTERCLAIMS TO INTERTRUST'S THIRD AMENDED COMPLAINT**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	

Defendant Microsoft Corporation ("Microsoft") answers the Third Amended Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

1. Microsoft admits that the Third Amended Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Third Amended Complaint.

2. Microsoft admits that the Third Amended Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Third Amended Complaint.

4. On information and belief, Microsoft admits the allegations of paragraph 4 of the Third Amended Complaint.

5. Microsoft admits the allegations of paragraph 5 of the Third Amended Complaint.

6. Microsoft admits, for purposes of this action only, that it transacts business in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the Third Amended Complaint.

7. Microsoft admits that on its face the title page of U.S. Patent No. 6,185,683 B1 ("the '683 Patent") states that it was issued February 6, 2001, is entitled "Trusted and secure techniques, systems and methods for item delivery and execution," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '683 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 7 of the Third Amended Complaint.

8. Microsoft admits that on its face the title page of U.S. Patent No. 6,253,193 B1 ("the '193 Patent") states that it was issued June 26, 2001, is entitled "Systems and methods for the secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corporation" as the assignee. Microsoft denies that the '193 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 8 of the Third Amended Complaint.

9. Microsoft admits that on its face the title page of U.S. Patent No. 5,940,504 ("the '504 Patent") states that it was issued August 17, 1999, and is entitled "Licensing management system and method in which datagrams including an address of a licensee and indicative of use of a licensed product are sent from the licensee's site." Microsoft denies that the '504 Patent was duly and lawfully issued. Microsoft lacks sufficient information to admit or deny any and all remaining allegations of paragraph 9 of the Third Amended Complaint.

10. Microsoft admits that on its face the title page of U.S. Patent No. 5,920,861 ("the '861 Patent") states that it was issued July 6, 1999, is entitled "Techniques for defining using and manipulating rights management data structures," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '861 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 10 of the Third Amended Complaint.

11. Microsoft admits that on its face the title page of U.S. Patent No. 5,892,900 ("the '900 Patent") states that it was issued April 6, 1999, is entitled "Systems and methods for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '900 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 11 of the Third Amended Complaint.

12. Microsoft admits that on its face the title page of U.S. Patent No. 5,982,891 ("the '891 Patent") states that it was issued November 9, 1999, is entitled "Systems and methods for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '891 Patent was duly and lawfully

issued. Microsoft further denies any and all remaining allegations of paragraph 12 of the Third Amended Complaint.

13. Microsoft admits that on its face the title page of U.S. Patent No. 5,917,912 ("the '912 Patent") states that it was issued June 29, 1999, is entitled "System and methods for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '912 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 13 of the Third Amended Complaint.

14. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Third Amended Complaint, as if fully restated herein.

15. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 15 of the Third Amended Complaint.

16. Microsoft denies any and all allegations of paragraph 16 of the Third Amended Complaint.

17. Microsoft denies any and all allegations of paragraph 17 of the Third Amended Complaint.

18. Microsoft denies any and all allegations of paragraph 18 of the Third Amended Complaint.

19. Microsoft denies any and all allegations of paragraph 19 of the Third Amended Complaint.

20. Microsoft denies any and all allegations of paragraph 20 of the Third Amended Complaint.

21. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 8 of the Third Amended Complaint, as if fully restated herein.

22. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now

infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 22 of the Third Amended Complaint.

23. Microsoft denies any and all allegations of paragraph 23 of the Third Amended Complaint.

24. Microsoft denies any and all allegations of paragraph 24 of the Third Amended Complaint.

25. Microsoft denies any and all allegations of paragraph 25 of the Third Amended Complaint.

26. Microsoft denies any and all allegations of paragraph 26 of the Third Amended Complaint.

27. Microsoft denies any and all allegations of paragraph 27 of the Third Amended Complaint.

28. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 9 of the Third Amended Complaint, as if fully restated herein.

29. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 29 of the Third Amended Complaint.

30. Microsoft denies any and all allegations of paragraph 30 of the Third Amended Complaint.

31. Microsoft denies any and all allegations of paragraph 31 of the Third Amended Complaint.

32. Microsoft denies any and all allegations of paragraph 32 of the Third Amended Complaint.

33. Microsoft denies any and all allegations of paragraph 33 of the Third Amended Complaint.

34. Microsoft denies any and all allegations of paragraph 34 of the Third Amended Complaint.

35. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 10 of the Third Amended Complaint, as if fully restated herein.

36. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 36 of the Third Amended Complaint.

37. Microsoft denies any and all allegations of paragraph 37 of the Third Amended Complaint.

38. Microsoft denies any and all allegations of paragraph 38 of the Third Amended Complaint.

39. Microsoft denies any and all allegations of paragraph 39 of the Third Amended Complaint.

40. Microsoft denies any and all allegations of paragraph 40 of the Third Amended Complaint.

41. Microsoft denies any and all allegations of paragraph 41 of the Third Amended Complaint.

42. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 11 of the Third Amended Complaint, as if fully restated herein.

43. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 43 of the Third Amended Complaint.

44. Microsoft denies any and all allegations of paragraph 44 of the Third Amended Complaint.

45. Microsoft denies any and all allegations of paragraph 45 of the Third Amended Complaint.

46. Microsoft denies any and all allegations of paragraph 46 of the Third Amended Complaint.

47. Microsoft denies any and all allegations of paragraph 47 of the Third Amended Complaint.

48. Microsoft denies any and all allegations of paragraph 48 of the Third Amended Complaint.

49. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 12 of the Third Amended Complaint, as if fully restated herein.

50. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 50 of the Third Amended Complaint.

51. Microsoft denies any and all allegations of paragraph 51 of the Third Amended Complaint.

52. Microsoft denies any and all allegations of paragraph 52 of the Third Amended Complaint.

53. Microsoft denies any and all allegations of paragraph 53 of the Third Amended Complaint.

54. Microsoft denies any and all allegations of paragraph 54 of the Third Amended Complaint.

55. Microsoft denies any and all allegations of paragraph 55 of the Third Amended Complaint.

56. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 13 of the Third Amended Complaint, as if fully restated herein.

57. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 57 of the Third Amended Complaint.

58. Microsoft denies any and all allegations of paragraph 58 of the Third Amended Complaint.

59. Microsoft denies any and all allegations of paragraph 59 of the Third Amended Complaint.

60. Microsoft denies any and all allegations of paragraph 60 of the Third Amended Complaint.

61. Microsoft denies any and all allegations of paragraph 61 of the Third Amended Complaint.

62. Microsoft denies any and all allegations of paragraph 62 of the Third Amended Complaint.

AFFIRMATIVE AND OTHER DEFENSES

Further answering the Third Amended Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patents

63. Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,185,683 B1 ("the '683 Patent"), U.S. Patent No. 6,253,193 B1 ("the '193 Patent"), U.S. Patent No. 5,940,504 ("the '504 Patent"), U.S. Patent No. 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), or U.S. Patent No. 5,917,912 ("the '912 Patent"), and is not liable for infringement thereof.

64. Any and all Microsoft products or methods that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent.

Second Defense: Invalidity of the Asserted Patents

65. On information and belief, the '683 Patent, the '193 Patent, the '504 Patent the '861 Patent, the '900 Patent, the '891 Patent, and the '912 Patent are invalid for failing to comply with the provisions of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailability of Relief

66. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 271(b) and (c) and is not entitled to any alleged damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent.

Fourth Defense: Unavailability of Relief

67. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent and any alleged infringement thereof.

Fifth Defense: Unavailability of Relief

68. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any damages.

Sixth Defense: Prosecution History Estoppel

69. Plaintiff's alleged causes of action for patent infringement are barred under the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

70. Plaintiff has dedicated to the public all methods, apparatus, and products disclosed in the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent, but not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture By/For United States Government

71. To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

72. To the extent that any of Plaintiff's allegations of infringement are premised on the alleged use, sale, offer for sale, license or offer of license of products that were manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft by or to a licensee of InterTrust, such allegations are barred pursuant to license.

Tenth Defense: Acquiescence

73. Plaintiff has acquiesced in at least a substantial part of the Microsoft conduct alleged to infringe.

Eleventh Defense: Laches

74. Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

75. The '861 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '861 Patent, set forth below.

Thirteenth Defense: Inequitable Conduct

76. The '900 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '900 Patent, set forth below.

Fourteenth Defense: Unenforceability

77. The claims of the '891 Patent, the '912 Patent, the '861 Patent, the '683 Patent, the '193 Patent and the '900 Patent are unenforceable due to unclean hands, inequitable conduct and misuse and illegal extension of the patent right, including those acts and failures to act set forth in Count XI of Microsoft's Counterclaims, set forth below.

///

///

///

///

COUNTERCLAIMS

COUNT I - DECLARATORY JUDGMENT OF NONINFRINGEMENT

78. This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, et seq. This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

79. Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

80. On information and belief, Plaintiff /Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

81. InterTrust purports to be the owner of U.S. Patent Nos. 6,185,683 B1 ("the '683 Patent"), 6,253,193 B1 ("the '193 Patent"), 5,940,504 ("the '504 Patent"), 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), and U.S. Patent No. 5,917,912 ("the '912 Patent").

82. InterTrust alleges that Microsoft has infringed the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and the '912 Patent.

83. No Microsoft product has infringed, either directly or indirectly, any claim of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent, and Microsoft is not liable for infringement thereof.

84. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the infringement or noninfringement of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent.

COUNT II - DECLARATORY JUDGMENT OF INVALIDITY OF THE '683 PATENT

85. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

86. The '683 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

87. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '683 Patent are valid or invalid.

COUNT III - DECLARATORY JUDGMENT OF INVALIDITY OF THE '193 PATENT

88. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

89. The '193 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

90. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '193 Patent are valid or invalid.

COUNT IV - DECLARATORY JUDGMENT OF INVALIDITY OF THE '504 PATENT

91. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

92. The '504 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the ~~Patent Laws, including one or more~~ of 35 U.S.C. §§ 102, 103 and 112.

93. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '504 Patent are valid or invalid.

COUNT V - DECLARATORY JUDGMENT OF INVALIDITY OF THE '861 PATENT

94. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

95. The '861 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

96. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are valid or invalid.

COUNT VI - DECLARATORY JUDGMENT OF INVALIDITY OF THE '900 PATENT

97. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

98. The '900 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

99. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are valid or invalid.

COUNT VII - DECLARATORY JUDGMENT OF INVALIDITY OF THE '891 PATENT

100. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

101. The '891 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

102. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '891 Patent are valid or invalid.

COUNT VIII - DECLARATORY JUDGMENT OF INVALIDITY OF THE '912 PATENT

103. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

104. The '912 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

105. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '912 Patent are valid or invalid.

COUNT IX - DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '861 PATENT

106. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

107. Claims 1-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, were not and are not entitled to the benefit of any application filing date prior to February 25, 1997, under 35 U.S.C. § 120 or otherwise.

108. "Exhibit A" refers to the document attached as Exhibit A to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a reprint of an article entitled "DigiBox: A Self-Protecting Container for Information Commerce").

109. On information and belief, the content of pages 2-14 of Exhibit A was presented at a public conference in the United States in July 1995.

110. "Exhibit B" refers to the document attached as Exhibit B to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a copy of a page from an International Application published under the Patent Cooperation Treaty (PCT), bearing International Publication Number WO 96/27155).

111. On information and belief, International Application WO 96/27155 has, at all times since its filing date, been owned and controlled by InterTrust or its predecessors in interest.

112. International Application WO 96/27155 (hereafter "the WO 96/27155 (PCT) publication") was published on September 6, 1996.

113. United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8, 1999, from a continuation of an application filed on February 13, 1995.

114. The Sibert article is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

115. The Sibert article is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. § 102(b).

116. The WO 96/27155 (PCT) publication is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

117. The WO 96/27155 (PCT) publication is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. § 102(a).

118. The '987 Patent is prior art to claims 29-129 of the '861 Patent application (SN 08/805,804).

119. The '987 Patent is prior art to claims 1-101 of the '861 Patent, under 35 U.S.C. § 102(e).

120. The Sibert article was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

121. The Sibert article was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

122. The WO 96/27155 (PCT) publication was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

123. The WO 96/27155 (PCT) publication was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

124. The '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804).

125. One or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the July 1995 publication of the Sibert article.

126. On information and belief, one or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

127. On information and belief, one or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the June 8, 1999 issuance of the '987 Patent.

128. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the July 1995 publication of the Sibert article.

129. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

130. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the June 8, 1999 issuance of the '987 Patent.

131. The applicants for the '861 Patent did not cite the Sibert article to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

132. The applicants for the '861 Patent did not cite the WO 96/27155 (PCT) publication to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

133. The applicants for the '861 Patent did not cite the '987 Patent to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

134. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the Sibert article.

135. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the WO 96/27155 (PCT) publication.

136. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the '987 Patent.

137. The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

138. The WO 96/27155 (PCT) publication is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

139. The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

140. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

141. InterTrust contends that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article discloses an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

142. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

143. InterTrust contends that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication discloses an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

144. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the Sibert article was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

145. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the WO 96/27155 (PCT) publication was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

146. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

147. The '861 Patent is unenforceable due to the inequitable conduct of the '861 Patent applicants and/or agents before the Patent and Trademark Office in connection with the '861 Patent application (SN 08/805,804).

148. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are enforceable.

COUNT X - DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '900 PATENT

149. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

150. The application and issued claims of the '900 Patent were not and are not entitled to the benefit of any application filing date prior to August 30, 1996, under 35 U.S.C. § 120 or otherwise.

151. Microsoft repeats and realleges paragraphs 31-32 of its Counterclaims, as if fully restated herein.

152. The Sibert article is prior art to the application and issued claims of the '900 Patent under 35 U.S.C. § 102(b).

153. The Sibert article was material to the patentability of application and issued claims of the '900 Patent, including, for example, issued claims 86 and 182.

154. One or more of the '900 Patent applicants knew of the July 1995 publication of the Sibert article while the '900 Patent application (SN 08/706,206) was pending.

155. On information and belief, one or more of the attorneys who prosecuted or assisted in the prosecution of the '900 Patent application (SN 08/706,206) knew of the July 1995 publication of the Sibert article while the '900 Patent application was pending.

156. The applicants for the '900 Patent did not cite the Sibert article to the Patent Office as prior art to any claims of the '900 Patent application (SN 08/706,206).

157. The applicants for the '900 Patent did not cite to the Patent Office as prior art to any claims of the '900 Patent application (SN 08/706,206) any reference having the same or substantially the same disclosure as the Sibert article.

158. The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the '900 Patent application (SN 08/706,206).

159. On information and belief, one or more of the '900 Patent applicants believed, during pendency of claim 1 of the '900 Patent application (SN 08/706,206), that the Sibert article disclosed an embodiment of claim 1 of the '900 Patent application (SN 08/706,206).

160. On information and belief, one or more of the '900 Patent applicants believed, while the '900 Patent application (SN 08/706,206) was pending, that the Sibert article was material to the patentability of various claims of the '900 Patent application (SN 08/706,206), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

161. The '900 Patent is unenforceable due to the inequitable conduct of the '900 Patent applicants before the Patent and Trademark Office in connection with the '900 Patent application (SN 08/706,206).

162. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are enforceable.

COUNT XI - DECLARATORY JUDGMENT OF UNENFORCEABILITY

163. Microsoft repeats and realleges paragraphs 1-5 and 30-85 of its Counterclaims, as if fully restated herein.

164. The '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent, and the '900 Patent are referred to as the Count XI Patents.

165. In prosecuting, marketing, and enforcing the Count XI Patents, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents. For example, InterTrust has accused non-infringing

products of infringement, has buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the particular claims in issue, and has buried the Examiners with hundreds or thousands of pages of redundant, verbose, unclear text, effectively prohibiting a real comparison of the alleged "invention" versus the prior art. This pattern of intentional conduct constitutes an abuse of the patent system, unclean hands, misuse and illegal extension of the patent right, rendering the Count XI patents unenforceable, as well as invalid under Section 112.

166. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent, and the '900 Patent are enforceable.

COUNT XII - INFRINGEMENT OF U.S. PATENT NO. 6,049,671

167. Microsoft repeats and realleges paragraphs 2-3 of its Counterclaims, as if fully restated herein.

168. This Court has exclusive subject matter jurisdiction over Microsoft's cause of action for patent infringement under Title 28, United States Code, Sections 1331 and 1338, and under the patent laws of the United States, Title 35 of the United States Code.

169. U.S. Patent No. 6,049,671 ("the '671 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on April 11, 2000.

170. A true copy of the '671 Patent is attached as Exhibit C to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

171. Microsoft owns all right, title and interest in the '671 Patent.

172. InterTrust has had actual notice of the '671 Patent.

173. InterTrust has infringed one or more claims of the '671 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

174. InterTrust's infringement of the '671 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

COUNT XIII - INFRINGEMENT
OF U.S. PATENT NO. 6,256,668

175. Microsoft repeats and realleges paragraphs 2-3 and 91 of its Counterclaims, as if fully restated herein.

176. U.S. Patent No. 6,256,668 B1 ("the '668 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on July 3, 2001.

177. A true copy of the '668 Patent is attached as Exhibit D to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

178. Microsoft owns all right, title and interest in the '668 Patent.

179. InterTrust has had actual notice of the '668 Patent.

180. InterTrust has infringed one or more claims of the '668 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

181. InterTrust's infringement of the '668 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A. The Court enter judgment against InterTrust, and dismiss with prejudice, any and all claims of the Third Amended Complaint;

B. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '683 Patent;

C. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '193 Patent;

D. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '504 Patent;

E. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '861 Patent;

F. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '900 Patent;

G. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '891 Patent;

H. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '912 Patent;

I. The Court enter judgment declaring that the '683 Patent is invalid;

J. The Court enter judgment declaring that the '193 Patent is invalid;

K. The Court enter judgment declaring that the '504 Patent is invalid;

L. The Court enter judgment declaring that the '861 Patent is invalid;

M. The Court enter judgment declaring that the '900 Patent is invalid;

N. The Court enter judgment declaring that the '891 Patent is invalid;

O. The Court enter judgment declaring that the '912 Patent is invalid;

P. The Court enter judgment declaring that the '861 Patent is unenforceable due to inequitable conduct;

Q. The Court enter judgment declaring that the '900 Patent is unenforceable due to inequitable conduct;

R. The Court enter judgment declaring that each of the '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent and the '900 Patent is unenforceable due to an abuse of the patent system, unclean hands, and misuse and illegal extension of the patent right;

S. The Court enter judgment that InterTrust has infringed the '671 Patent;

T. The Court enter judgment that InterTrust has infringed the '668 Patent;

U. The Court enter a permanent injunction prohibiting InterTrust, its officers, agents, servants, employees, and all persons in active concert or participation with any of them from infringing the '671 and '668 Patents;

///

V. The Court award damages and attorney fees against InterTrust pursuant to the provisions of 35 U.S.C §§ 284 and 285.

W. The Court award to Microsoft pre-judgment interest and the costs of this action.

X. The Court award to Microsoft its reasonable costs and attorneys' fees; and

Y. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

DATED: November 14, 2001

By:
WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
Microsoft Corporation

Of Counsel:

T. ANDREW CULBERT, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

DECLARATION OF SERVICE VIA ELECTRONIC MAIL AND U.S. MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 1000 Marsh Road, Menlo Park, California 94025.

On November 14, 2001, I served:

MICROSOFT CORPORATION'S AMENDED ANSWER AND COUNTERCLAIMS TO INTERTRUST'S THIRD AMENDED COMPLAINT

By transmitting a copy of the above-listed document(s) in PDF form via electronic mail **Michael H. Page at mhp@kvn.com, Christopher P. Isaac at chris.isaac@finnegan.com, Stephen E. Taylor at staylor@tcolaw.com** and **James E. Geringer** at **james.geringer@klarquist.com** and also by placing true and correct copies of the above documents in an envelope addressed to:

John W. Keker, Esq.
Michael H. Page, Esq.
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111
Tel. No. 415-391-5400
Fax No. 415-397-7188
Email: jwk@kvn.com
Email: mhp@kvn.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Christopher P. Isaac, Esq.
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER LLP
1300 I. Street, N.W.
Washington, DC 20005-3314
Tel. No. 202-408-4000
Fax No. 202-408-4400
Email: chris.isaac@finnegan.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Stephen E. Taylor, Esq.
TAYLOR & CO. LAW OFFICES
1050 Marina Village Parkway, Suite 101
Alameda, CA 94501
Tel. No. 510-865-9401
Fax No. 510-865-9408
Email: staylor@tcolaw.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

John D. Vandenberg, Esq.
James E. Geringer, Esq.
KLARQUIST, SPARKMAN, CAMPBELL,
LEIGH & WHINSTON LLP
One World Trade Center
121 S. W. Salmon Street, Suite 1600
Portland, Oregon 97204
Tel. No: 503-226-7391
Fax No: 503-228-9446
Email: john.vandenberg@klarquist.com
Email: james.geringer@klarquist.com

Attorneys for Defendant and
Counterclaimant, MICROSOFT
CORPORATION

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Menlo Park, California.

Executed on November 14, 2001 at Menlo Park, California.

I declare under penalty of perjury that the foregoing is true and correct.

____
(SIGNATURE)

____
(PRINT NAME)

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	CASE NO. C01-1640 SBA **MICROSOFT CORPORATION'S *"CORRECTED"* AMENDED ANSWER AND COUNTERCLAIMS TO INTERTRUST'S THIRD AMENDED COMPLAINT**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	

Defendant Microsoft Corporation ("Microsoft") answers the Third Amended Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

1. Microsoft admits that the Third Amended Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Third Amended Complaint.

2. Microsoft admits that the Third Amended Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Third Amended Complaint.

4. On information and belief, Microsoft admits the allegations of paragraph 4 of the Third Amended Complaint.

5. Microsoft admits the allegations of paragraph 5 of the Third Amended Complaint.

6. Microsoft admits, for purposes of this action only, that it transacts business in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the Third Amended Complaint.

7. Microsoft admits that on its face the title page of U.S. Patent No. 6,185,683 B1 ("the '683 Patent") states that it was issued February 6, 2001, is entitled "Trusted and secure techniques, systems and methods for item delivery and execution," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '683 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 7 of the Third Amended Complaint.

issued. Microsoft further denies any and all remaining allegations of paragraph 12 of the Third Amended Complaint.

13. Microsoft admits that on its face the title page of U.S. Patent No. 5,917,912 ("the '912 Patent") states that it was issued June 29, 1999, is entitled "System and methods for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '912 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 13 of the Third Amended Complaint.

14. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Third Amended Complaint, as if fully restated herein.

15. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 15 of the Third Amended Complaint.

16. Microsoft denies any and all allegations of paragraph 16 of the Third Amended Complaint.

17. Microsoft denies any and all allegations of paragraph 17 of the Third Amended Complaint.

18. Microsoft denies any and all allegations of paragraph 18 of the Third Amended Complaint.

19. Microsoft denies any and all allegations of paragraph 19 of the Third Amended Complaint.

20. Microsoft denies any and all allegations of paragraph 20 of the Third Amended Complaint.

21. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 8 of the Third Amended Complaint, as if fully restated herein.

22. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now

infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 22 of the Third Amended Complaint.

23. Microsoft denies any and all allegations of paragraph 23 of the Third Amended Complaint.

24. Microsoft denies any and all allegations of paragraph 24 of the Third Amended Complaint.

25. Microsoft denies any and all allegations of paragraph 25 of the Third Amended Complaint.

26. Microsoft denies any and all allegations of paragraph 26 of the Third Amended Complaint.

27. Microsoft denies any and all allegations of paragraph 27 of the Third Amended Complaint.

28. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 9 of the Third Amended Complaint, as if fully restated herein.

29. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 29 of the Third Amended Complaint.

30. Microsoft denies any and all allegations of paragraph 30 of the Third Amended Complaint.

31. Microsoft denies any and all allegations of paragraph 31 of the Third Amended Complaint.

32. Microsoft denies any and all allegations of paragraph 32 of the Third Amended Complaint.

33. Microsoft denies any and all allegations of paragraph 33 of the Third Amended Complaint.

34. Microsoft denies any and all allegations of paragraph 34 of the Third Amended Complaint.

35. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 10 of the Third Amended Complaint, as if fully restated herein.

36. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 36 of the Third Amended Complaint.

37. Microsoft denies any and all allegations of paragraph 37 of the Third Amended Complaint.

38. Microsoft denies any and all allegations of paragraph 38 of the Third Amended Complaint.

39. Microsoft denies any and all allegations of paragraph 39 of the Third Amended Complaint.

40. Microsoft denies any and all allegations of paragraph 40 of the Third Amended Complaint.

41. Microsoft denies any and all allegations of paragraph 41 of the Third Amended Complaint.

42. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 11 of the Third Amended Complaint, as if fully restated herein.

43. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 43 of the Third Amended Complaint.

44. Microsoft denies any and all allegations of paragraph 44 of the Third Amended Complaint.

45. Microsoft denies any and all allegations of paragraph 45 of the Third Amended Complaint.

46. Microsoft denies any and all allegations of paragraph 46 of the Third Amended Complaint.

47. Microsoft denies any and all allegations of paragraph 47 of the Third Amended Complaint.

48. Microsoft denies any and all allegations of paragraph 48 of the Third Amended Complaint.

49. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 12 of the Third Amended Complaint, as if fully restated herein.

50. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 50 of the Third Amended Complaint.

51. Microsoft denies any and all allegations of paragraph 51 of the Third Amended Complaint.

52. Microsoft denies any and all allegations of paragraph 52 of the Third Amended Complaint.

53. Microsoft denies any and all allegations of paragraph 53 of the Third Amended Complaint.

54. Microsoft denies any and all allegations of paragraph 54 of the Third Amended Complaint.

55. Microsoft denies any and all allegations of paragraph 55 of the Third Amended Complaint.

56. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 13 of the Third Amended Complaint, as if fully restated herein.

57. Microsoft admits that the Third Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Third Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 57 of the Third Amended Complaint.

58. Microsoft denies any and all allegations of paragraph 58 of the Third Amended Complaint.

59. Microsoft denies any and all allegations of paragraph 59 of the Third Amended Complaint.

60. Microsoft denies any and all allegations of paragraph 60 of the Third Amended Complaint.

61. Microsoft denies any and all allegations of paragraph 61 of the Third Amended Complaint.

62. Microsoft denies any and all allegations of paragraph 62 of the Third Amended Complaint.

AFFIRMATIVE AND OTHER DEFENSES

Further answering the Third Amended Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patents

63. Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,185,683 B1 ("the '683 Patent"), U.S. Patent No. 6,253,193 B1 ("the '193 Patent"), U.S. Patent No. 5,940,504 ("the '504 Patent"), U.S. Patent No. 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), or U.S. Patent No. 5,917,912 ("the '912 Patent"), and is not liable for infringement thereof.

64. Any and all Microsoft products or methods that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent.

Second Defense: Invalidity of the Asserted Patents

65. On information and belief, the '683 Patent, the '193 Patent, the '504 Patent the '861 Patent, the '900 Patent, the '891 Patent, and the '912 Patent are invalid for failing to comply with the provisions of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailability of Relief

66. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 271(b) and (c) and is not entitled to any alleged damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent.

Fourth Defense: Unavailability of Relief

67. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent and any alleged infringement thereof.

Fifth Defense: Unavailability of Relief

68. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any damages.

Sixth Defense: Prosecution History Estoppel

69. Plaintiff's alleged causes of action for patent infringement are barred under the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

70. Plaintiff has dedicated to the public all methods, apparatus, and products disclosed in the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent, but not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture By/For United States Government

71. To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

72. To the extent that any of Plaintiff's allegations of infringement are premised on the alleged use, sale, offer for sale, license or offer of license of products that were manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft by or to a licensee of InterTrust, such allegations are barred pursuant to license.

Tenth Defense: Acquiescence

73. Plaintiff has acquiesced in at least a substantial part of the Microsoft conduct alleged to infringe.

Eleventh Defense: Laches

74. Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

75. The '861 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '861 Patent, set forth below.

Thirteenth Defense: Inequitable Conduct

76. The '900 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '900 Patent, set forth below.

Fourteenth Defense: Unenforceability

77. The claims of the '891 Patent, the '912 Patent, the '861 Patent, the '683 Patent, the '193 Patent and the '900 Patent are unenforceable due to unclean hands, inequitable conduct and misuse and illegal extension of the patent right, including those acts and failures to act set forth in Count XI of Microsoft's Counterclaims, set forth below.

///

///

///

///

COUNTERCLAIMS

COUNT I - DECLARATORY JUDGMENT OF NONINFRINGEMENT

1. This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, et seq. This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

2. Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

3. On information and belief, Plaintiff /Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

4. InterTrust purports to be the owner of U.S. Patent Nos. 6,185,683 B1 ("the '683 Patent"), 6,253,193 B1 ("the '193 Patent"), 5,940,504 ("the '504 Patent"), 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), and U.S. Patent No. 5,917,912 ("the '912 Patent").

5. InterTrust alleges that Microsoft has infringed the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and the '912 Patent.

6. No Microsoft product has infringed, either directly or indirectly, any claim of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, or the '912 Patent, and Microsoft is not liable for infringement thereof.

7. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the infringement or noninfringement of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, and/or the '912 Patent.

COUNT II - DECLARATORY JUDGMENT OF INVALIDITY OF THE '683 PATENT

8. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

9. The '683 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

10. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '683 Patent are valid or invalid.

COUNT III - DECLARATORY JUDGMENT OF INVALIDITY OF THE '193 PATENT

11. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

12. The '193 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

13. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '193 Patent are valid or invalid.

COUNT IV - DECLARATORY JUDGMENT OF INVALIDITY OF THE '504 PATENT

14. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

15. The '504 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

16. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '504 Patent are valid or invalid.

COUNT V - DECLARATORY JUDGMENT OF INVALIDITY OF THE '861 PATENT

17. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

18. The '861 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

19. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are valid or invalid.

COUNT VI - DECLARATORY JUDGMENT OF INVALIDITY OF THE '900 PATENT

20. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

21. The '900 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

22. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are valid or invalid.

COUNT VII - DECLARATORY JUDGMENT OF INVALIDITY OF THE '891 PATENT

23. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

24. The '891 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

25. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '891 Patent are valid or invalid.

COUNT VIII - DECLARATORY JUDGMENT OF INVALIDITY OF THE '912 PATENT

26. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated herein.

27. The '912 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

28. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '912 Patent are valid or invalid.

COUNT IX - DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '861 PATENT

29. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

30. Claims 1-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, were not and are not entitled to the benefit of any application filing date prior to February 25, 1997, under 35 U.S.C. § 120 or otherwise.

31. "Exhibit A" refers to the document attached as Exhibit A to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a reprint of an article entitled "DigiBox: A Self-Protecting Container for Information Commerce").

32. On information and belief, the content of pages 2-14 of Exhibit A was presented at a public conference in the United States in July 1995.

33. "Exhibit B" refers to the document attached as Exhibit B to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a copy of a page from an International Application published under the Patent Cooperation Treaty (PCT), bearing International Publication Number WO 96/27155).

34. On information and belief, International Application WO 96/27155 has, at all times since its filing date, been owned and controlled by InterTrust or its predecessors in interest.

35. International Application WO 96/27155 (hereafter "the WO 96/27155 (PCT) publication") was published on September 6, 1996.

36. United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8, 1999, from a continuation of an application filed on February 13, 1995.

37. The Sibert article is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

38. The Sibert article is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. § 102(b).

39. The WO 96/27155 (PCT) publication is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

40. The WO 96/27155 (PCT) publication is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. § 102(a).

41. The '987 Patent is prior art to claims 29-129 of the '861 Patent application (SN 08/805,804).

42. The '987 Patent is prior art to claims 1-101 of the '861 Patent, under 35 U.S.C. § 102(e).

43. The Sibert article was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

44. The Sibert article was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

45. The WO 96/27155 (PCT) publication was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

46. The WO 96/27155 (PCT) publication was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

47. The '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804).

48. One or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the July 1995 publication of the Sibert article.

49. On information and belief, one or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

50. On information and belief, one or more of the '861 Patent applicants knew, while the '861 Patent application (SN 08/805,804) was pending, of the June 8, 1999 issuance of the '987 Patent.

51. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the July 1995 publication of the Sibert article.

52. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the September 1996 publication of the WO 96/27155 (PCT) publication.

53. One or more of the attorneys who prosecuted or assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application was pending, of the June 8, 1999 issuance of the '987 Patent.

54. The applicants for the '861 Patent did not cite the Sibert article to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

55. The applicants for the '861 Patent did not cite the WO 96/27155 (PCT) publication to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

56. The applicants for the '861 Patent did not cite the '987 Patent to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

57. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the Sibert article.

58. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the WO 96/27155 (PCT) publication.

59. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the '987 Patent.

60. The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

61. The WO 96/27155 (PCT) publication is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

62. The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

63. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

64. InterTrust contends that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article discloses an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

65. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

66. InterTrust contends that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication discloses an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

67. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the Sibert article was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

68. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the WO 96/27155 (PCT) publication was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

69. On information and belief, one or more of the '861 Patent applicants believed, while the '861 Patent application (SN 08/805,804) was pending, that the '987 Patent was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

70. The '861 Patent is unenforceable due to the inequitable conduct of the '861 Patent applicants and/or agents before the Patent and Trademark Office in connection with the '861 Patent application (SN 08/805,804).

71. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are enforceable.

COUNT X - DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '900 PATENT

72. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

73. The application and issued claims of the '900 Patent were not and are not entitled to the benefit of any application filing date prior to August 30, 1996, under 35 U.S.C. § 120 or otherwise.

74. Microsoft repeats and realleges paragraphs 31-32 of its Counterclaims, as if fully restated herein.

75. The Sibert article is prior art to the application and issued claims of the '900 Patent under 35 U.S.C. § 102(b).

76. The Sibert article was material to the patentability of application and issued claims of the '900 Patent, including, for example, issued claims 86 and 182.

77. One or more of the '900 Patent applicants knew of the July 1995 publication of the Sibert article while the '900 Patent application (SN 08/706,206) was pending.

78. On information and belief, one or more of the attorneys who prosecuted or assisted in the prosecution of the '900 Patent application (SN 08/706,206) knew of the July 1995 publication of the Sibert article while the '900 Patent application was pending.

79. The applicants for the '900 Patent did not cite the Sibert article to the Patent Office as prior art to any claims of the '900 Patent application (SN 08/706,206).

80. The applicants for the '900 Patent did not cite to the Patent Office as prior art to any claims of the '900 Patent application (SN 08/706,206) any reference having the same or substantially the same disclosure as the Sibert article.

81. The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the '900 Patent application (SN 08/706,206).

82. On information and belief, one or more of the '900 Patent applicants believed, during pendency of claim 1 of the '900 Patent application (SN 08/706,206), that the Sibert article disclosed an embodiment of claim 1 of the '900 Patent application (SN 08/706,206).

83. On information and belief, one or more of the '900 Patent applicants believed, while the '900 Patent application (SN 08/706,206) was pending, that the Sibert article was material to the patentability of various claims of the '900 Patent application (SN 08/706,206), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

84. The '900 Patent is unenforceable due to the inequitable conduct of the '900 Patent applicants before the Patent and Trademark Office in connection with the '900 Patent application (SN 08/706,206).

85. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are enforceable.

COUNT XI - DECLARATORY JUDGMENT OF UNENFORCEABILITY

86. Microsoft repeats and realleges paragraphs 1-5 and 30-85 of its Counterclaims, as if fully restated herein.

87. The '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent, and the '900 Patent are referred to as the Count XI Patents.

88. In prosecuting, marketing, and enforcing the Count XI Patents, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents. For example, InterTrust has accused non-infringing

products of infringement, has buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the particular claims in issue, and has buried the Examiners with hundreds or thousands of pages of redundant, verbose, unclear text, effectively prohibiting a real comparison of the alleged "invention" versus the prior art. This pattern of intentional conduct constitutes an abuse of the patent system, unclean hands, misuse and illegal extension of the patent right, rendering the Count XI patents unenforceable, as well as invalid under Section 112.

89. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent, and the '900 Patent are enforceable.

COUNT XII - INFRINGEMENT OF U.S. PATENT NO. 6,049,671

90. Microsoft repeats and realleges paragraphs 2-3 of its Counterclaims, as if fully restated herein.

91. This Court has exclusive subject matter jurisdiction over Microsoft's cause of action for patent infringement under Title 28, United States Code, Sections 1331 and 1338, and under the patent laws of the United States, Title 35 of the United States Code.

92. U.S. Patent No. 6,049,671 ("the '671 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on April 11, 2000.

93. A true copy of the '671 Patent is attached as Exhibit C to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

94. Microsoft owns all right, title and interest in the '671 Patent.

95. InterTrust has had actual notice of the '671 Patent.

96. InterTrust has infringed one or more claims of the '671 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

97. InterTrust's infringement of the '671 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

COUNT XIII - INFRINGEMENT OF U.S. PATENT NO. 6,256,668

98. Microsoft repeats and realleges paragraphs 2-3 and 91 of its Counterclaims, as if fully restated herein.

99. U.S. Patent No. 6,256,668 B1 ("the '668 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on July 3, 2001.

100. A true copy of the '668 Patent is attached as Exhibit D to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

101. Microsoft owns all right, title and interest in the '668 Patent.

102. InterTrust has had actual notice of the '668 Patent.

103. InterTrust has infringed one or more claims of the '668 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

104. InterTrust's infringement of the '668 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A. The Court enter judgment against InterTrust, and dismiss with prejudice, any and all claims of the Third Amended Complaint;

B. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '683 Patent;

C. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '193 Patent;

D. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '504 Patent;

E. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '861 Patent;

F. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '900 Patent;

G. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '891 Patent;

H. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '912 Patent;

I. The Court enter judgment declaring that the '683 Patent is invalid;

J. The Court enter judgment declaring that the '193 Patent is invalid;

K. The Court enter judgment declaring that the '504 Patent is invalid;

L. The Court enter judgment declaring that the '861 Patent is invalid;

M. The Court enter judgment declaring that the '900 Patent is invalid;

N. The Court enter judgment declaring that the '891 Patent is invalid;

O. The Court enter judgment declaring that the '912 Patent is invalid;

P. The Court enter judgment declaring that the '861 Patent is unenforceable due to inequitable conduct;

Q. The Court enter judgment declaring that the '900 Patent is unenforceable due to inequitable conduct;

R. The Court enter judgment declaring that each of the '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent and the '900 Patent is unenforceable due to an abuse of the patent system, unclean hands, and misuse and illegal extension of the patent right;

S. The Court enter judgment that InterTrust has infringed the '671 Patent;

T. The Court enter judgment that InterTrust has infringed the '668 Patent;

U. The Court enter a permanent injunction prohibiting InterTrust, its officers, agents, servants, employees, and all persons in active concert or participation with any of them from infringing the '671 and '668 Patents;

///

V. The Court award damages and attorney fees against InterTrust pursuant to the provisions of 35 U.S.C §§ 284 and 285.

W. The Court award to Microsoft pre-judgment interest and the costs of this action.

X. The Court award to Microsoft its reasonable costs and attorneys' fees; and

Y. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

DATED: November 15, 2001

By:____________________________
WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
Microsoft Corporation

Of Counsel:

T. Andrew Culbert, Esq.
MICROSOFT CORPORATION
One Microsoft Way, Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

DECLARATION OF SERVICE VIA ELECTRONIC MAIL AND U.S. MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 1000 Marsh Road, Menlo Park, California 94025.

On November 15, 2001, I served:

MICROSOFT CORPORATION'S *"CORRECTED"* AMENDED ANSWER AND COUNTERCLAIMS TO INTERTRUST'S THIRD AMENDED COMPLAINT

By transmitting a copy of the above-listed document(s) in PDF form via electronic mail **Michael H. Page at mhp@kvn.com, Christopher P. Isaac at chris.isaac@finnegan.com, Stephen E. Taylor at staylor@tcolaw.com** and **James E. Geringer at james.geringer@klarquist.com** and also by placing true and correct copies of the above documents in an envelope addressed to:

John W. Keker, Esq.
Michael H. Page, Esq.
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111
Tel. No. 415-391-5400
Fax No. 415-397-7188
Email: jwk@kvn.com
Email: mhp@kvn.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Christopher P. Isaac, Esq.
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER LLP
1300 I. Street, N.W.
Washington, DC 20005-3314
Tel. No. 202-408-4000
Fax No. 202-408-4400
Email: chris.isaac@finnegan.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Stephen E. Taylor, Esq.
TAYLOR & CO. LAW OFFICES
1050 Marina Village Parkway, Suite 101
Alameda, CA 94501
Tel. No. 510-865-9401
Fax No. 510-865-9408
Email: staylor@tcolaw.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

John D. Vandenberg, Esq.
James E. Geringer, Esq.
KLARQUIST, SPARKMAN, CAMPBELL,
LEIGH & WHINSTON LLP
One World Trade Center
121 S. W. Salmon Street, Suite 1600
Portland, Oregon 97204
Tel. No: 503-226-7391
Fax No: 503-228-9446
Email: john.vandenberg@klarquist.com
Email: james.geringer@klarquist.com

Attorneys for Defendant and
Counterclaimant, MICROSOFT
CORPORATION

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Menlo Park, California.

Executed on November 15, 2001 at Menlo Park, California.

I declare under penalty of perjury that the foregoing is true and correct.

____
(SIGNATURE)

____
(PRINT NAME)

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
MICHAEL H. PAGE - #154913
L. JAY KUO - #173293
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
CHRISTOPHER P. ISAAC
1300 I Street, N.W.
Washington, D.C. 20005-3314
Telephone: (202) 408-4000
Facsimile: (202) 408-4400

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES
CORPORATION,
a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a
Washington corporation,

Defendant.

C 02 0647
EDL

COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NO. 6,157,721

DEMAND FOR JURY TRIAL

Plaintiff INTERTRUST TECHNOLOGIES CORPORATION (hereafter "InterTrust") hereby complains of Defendant MICROSOFT CORPORATION (hereafter "Microsoft"), and alleges as follows:

JURISDICTION AND VENUE

1. This action for patent infringement arises under the patent laws of the United States, Title 35, United States Code, more particularly 35 U.S.C. §§ 271 and 281.

2. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(c) and 1400(b).

THE PARTIES

4. Plaintiff InterTrust is a Delaware corporation with its principal place of business at 4750 Patrick Henry Drive, Santa Clara, California.

5. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft is a Washington Corporation with its principal place of business at One Microsoft Way, Redmond, Washington.

6. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft does business in this judicial district and has committed and is continuing to commit acts of infringement in this judicial district.

7. InterTrust is the owner of United States Patent No. 6,157,721, entitled "Systems and methods using cryptography to protect secure computing environments" ("the '721 patent"), duly and lawfully issued on December 5, 2000.

FIRST CLAIM FOR RELIEF

8. InterTrust hereby incorporates by reference paragraphs 1-7 as if restated herein.

9. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

10. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '721 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '721 patent under §271(a) will continue unless enjoined by this Court.

11. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '721 patent under § 271(a), thereby inducing infringement of the '721 patent under § 271(b). InterTrust is further

informed and believes, and on that basis alleges, that Microsoft's infringement of the '721 patent under §271(b) will continue unless enjoined by this Court.

12. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '721 patent under § 271(c) by providing software and related functions especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '721 patent under §271(c) will continue unless enjoined by this Court.

13. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '721 patent in the manner described above in paragraphs 10 through 12, and will continue to do so unless enjoined by this Court.

14. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement, gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, InterTrust prays for relief as follows:

A. That Microsoft be adjudged to have infringed the '721 patent under 35 U.S.C. § 271(a);

B. That Microsoft be adjudged to have infringed the '721 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '721 patent under 35 U.S.C. § 271(a);

C. That Microsoft be adjudged to have contributorily infringed the '721 patent under 35 U.S.C. § 271(c);

D. That Microsoft be adjudged to have willfully infringed the '721 patent under 35 U.S.C. §§ 271(a), (b), and (c);

E. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '721 patent;

F. That this Court assess pre-judgment and post-judgment interest and costs against Microsoft, and award such interest and costs to InterTrust, pursuant to 35 U.S.C. § 284; and

G. That InterTrust have such other and further relief as the Court may deem proper.

Dated: February 6, 2002

KEKER & VAN NEST, LLP

By:_________________________
MICHAEL H. PAGE
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

DEMAND FOR JURY TRIAL

Plaintiff InterTrust herby demands a trial by jury as to all issues triable by jury, specifically including, but not limited to, the issue of infringement of United States Patent No. 6,157,721.

Dated: February 6, 2002

KEKER & VAN NEST, LLP

By:______________________________
MICHAEL H. PAGE
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

WILLIAM L. ANTHONY, JR. (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE (State Bar No. 178960)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington Corporation, Defendant.	CASE NO: C 02 0647 SBA **MICROSOFT CORPORATION'S ANSWER AND COUNTERCLAIMS** **(JURY TRIAL DEMANDED)**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter-Defendant.	

Defendant Microsoft Corporation ("Microsoft") answers the Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

Microsoft admits that the Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patent asserted against Microsoft in the Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Complaint.

1. Microsoft admits that the Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

2. Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Complaint.

3. Upon information and belief, Microsoft admits the allegations of paragraph 4 of the Complaint.

4. Microsoft admits the allegations of paragraph 5 of the Complaint.

5. Microsoft admits, for purposes of this action only, that it transacts business in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the Complaint.

6. Microsoft admits that on its face the title page of U.S. Patent No. 6,157,721 ("the '721 Patent") states that it was issued December 5, 2000, is entitled "Systems and methods using cryptography to protect secure computing environments," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '721 Patent was duly and lawfully issued. Microsoft further denies, or lacks information or belief sufficient to admit or deny any and all remaining allegations of paragraph 7 of the Complaint.

7. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Complaint, as if fully restated herein.

8. Microsoft admits that the Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patent

asserted against Microsoft in the Complaint. Microsoft denies any and all remaining allegations of paragraph 9 of the Complaint.

9. Microsoft denies, or lacks information and belief sufficient to admit or deny as to InterTrust's claim as to any and all allegations of paragraph 10 of the Complaint.

10. Microsoft denies any and all allegations of paragraph 11 of the Complaint.

11. Microsoft denies any and all allegations of paragraph 12 of the Complaint.

12. Microsoft denies any and all allegations of paragraph 13 of the Complaint.

13. Microsoft denies any and all allegations of paragraph 14 of the Complaint.

AFFIRMATIVE AND OTHER DEFENSES

Further answering the Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patent

Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,157,721 ("the '721 Patent"), and is not liable for infringement thereof.

Any and all Microsoft products or actions that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '721 Patent.

Second Defense: Invalidity of the Asserted Patent

On information and belief, the '721 Patent is invalid for failing to comply with the provisions of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailability of Relief

On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 271(b) and is not entitled to any alleged damages prior to providing any actual notice to Microsoft of the '721 Patent.

Fourth Defense: Unavailability of Relief

On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to providing any actual notice to Microsoft of the '721 Patent, and any alleged infringement thereof.

Fifth Defense: Unavailability of Relief

On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any damages.

Sixth Defense: Prosecution History Estoppel

Plaintiff's alleged cause of action for patent infringement is barred under the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '721 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

Plaintiff has dedicated to the public all methods, apparatus, and products disclosed in the '721 Patent, but not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture By/For United States Government

To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

To the extent that Plaintiff's allegation of infringement is premised on the alleged use, sale, or offer for sale of a product that was manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft to or by a licensee of InterTrust, such allegation is barred pursuant to license.

Tenth Defense: Acquiescence

Plaintiff has acquiesced in at least those acts of Microsoft that are alleged to infringe the '721 Patent.

Eleventh Defense: Laches

Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

The '721 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Count III of Microsoft's Counterclaims, set forth below.

Thirteenth Defense: Unenforceability

The claims of the '721 Patent are unenforceable due to unclean hands, inequitable conduct and misuse and illegal extension of the patent right, including those acts and failures to act set forth in Count IV of Microsoft's Counterclaims, set forth below.

COUNTERCLAIMS
COUNT I – DECLARATORY JUDGMENT OF NONINFRINGEMENT

1. This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, *et seq.* This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

2. Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

3. On information and belief, Plaintiff /Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

4. InterTrust purports to be the owner of U.S. Patent No. 6,157,721 ("the '721 Patent").

5. InterTrust alleges that Microsoft has infringed the '721 Patent.

6. InterTrust issued a press release on February 7, 2002. The press release stated that InterTrust had filed a law suit against Microsoft for patent infringement. The press release specificed that InterTrust "alleges infringement by Microsoft's 'Plug and Play' Driver Certification Program."

7. Microsoft's certification of hardware drivers has not infringed, either directly or indirectly, any claim of the '721 Patent, and Microsoft is not liable for infringement thereof.

8. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the infringement or noninfringement of the '721 Patent.

COUNT II – DECLARATORY JUDGMENT OF INVALIDITY OF THE '721 PATENT

9. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

10. The '721 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

11. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are valid or invalid.

COUNT III – DECLARATORY JUDGMENT OF UNENFORDEABILITY OF THE '721 PATENT

12. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

13. Claims 1-43 of the '721 Patent application (SN 08/689,754), and claims 1-41 of the '721 Patent, were not and are not entitled to the benefit of any application filing date prior to August 12, 1996, under 35 U.S.C. § 120 or otherwise.

14. United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8, 1999, from a continuation of an application filed on February 13, 1995.

15. The '987 Patent is prior art to claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754).

16. The '987 Patent is prior art to claims 1-41 of the '721 Patent under 35 U.S.C. § 102(e).

17. The '987 Patent was material to the patentability of claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754).

18. One or more of the '721 Patent applicants knew, while the '721 Patent application (SN 08/689,754) was pending, of the '987 Patent.

19. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '721 Patent application (SN 08/689,754) knew, while that application was pending, of the '987 Patent.

20. The applicants for the '721 Patent did not cite the '987 Patent to the Patent Office as prior art to any of claims 1-43 of the '721 Patent application (SN 08/689,754).

21. The applicants for the '721 Patent did not cite to the Patent Office as prior art to any of claims 1-43 of the '721 Patent application (SN 08/689,754) any reference having the same or substantially the same disclosure as the '987 Patent.

22. The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '721 Patent application (SN 08/689,754).

23. On information and belief, one or more of the '721 Patent applicants believed, while the '721 Patent application (SN 08/689,754) was pending, that the '987 Patent was material to the patentability of one or more of claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

24. The '721 Patent is unenforceable due to the inequitable conduct of the '721 Patent applicants and/or agents before the Patent and Trademark Office in connection with the '721 Patent application (SN 08/689,754).

25. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are enforceable.

COUNT IV – DECLARATORY JUDGMENT OF UNENFORCEABILITY

26. Microsoft repeats and realleges paragraphs 1-5 and 12-24 of its Counterclaims, as if fully restated herein.

27. In prosecuting, marketing, and enforcing various related patents, including the '721 Patent, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents. For example, InterTrust has accused non-infringing products of infringement, has buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the particular claims in issue, and has buried the Examiners with hundreds or thousands of pages of redundant, verbose, unclear text, effectively prohibiting a real comparison of the alleged "invention" versus the prior art. This pattern of intentional conduct constitutes an abuse of the patent system, unclean hands, misuse and illegal extension of the patent right, rendering the '721 Patent unenforceable, as well as invalid under Section 112.

28. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are enforceable.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A. The Court enter judgment against InterTrust, and dismiss with prejudice, any and all claims of the Complaint;

B. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '721 Patent;

C. The Court enter judgment declaring that the '721 Patent is invalid;

D. The Court enter judgment declaring that the '721 Patent is unenforceable due to inequitable conduct;

E. The Court enter judgment declaring that the '721 Patent is unenforceable due to abuse of the patent system, unclean hands, and misuse and illegal extension of the patent right;

F. The Court award attorney fees against InterTrust pursuant to the provisions of 35 U.S.C § 285;

G. The Court award to Microsoft pre-judgment interest and the costs of this actions;

H. The Court award to Microsoft its reasonable costs and attorneys' fees; and

I. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

Dated: March 25, 2002

By: Heidi Keefe

WILLIAM L. ANTHONY
ERIC L. WESENBERG
HEIDI L. KEEFE
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant/Counterclaimant
MICROSOFT CORPORATION

Of Counsel:

T. Andrew Culbert, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Telephone: (425) 936-6921

WILLIAM L. ANTHONY, JR. (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE (State Bar No. 178960)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN R. ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington Corporation, Defendant.	CASE NO: C 02 0647 SBA **MICROSOFT CORPORATION'S FIRST AMENDED ANSWER AND COUNTERCLAIMS**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter-Defendant.	

Defendant Microsoft Corporation ("Microsoft") answers the Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

1. Microsoft admits that the Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patent asserted against Microsoft in the Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Complaint.

2. Microsoft admits that the Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Complaint.

4. Upon information and belief, Microsoft admits the allegations of paragraph 4 of the Complaint.

5. Microsoft admits the allegations of paragraph 5 of the Complaint.

6. Microsoft admits, for purposes of this action only, that it transacts business in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the Complaint.

7. Microsoft admits that on its face the title page of U.S. Patent No. 6,157,721 ("the '721 Patent") states that it was issued December 5, 2000, is entitled "Systems and methods using cryptography to protect secure computing environments," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '721 Patent was duly and lawfully issued. Microsoft further denies, or lacks information or belief sufficient to admit or deny any and all remaining allegations of paragraph 7 of the Complaint.

8. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Complaint, as if fully restated herein.

9. Microsoft admits that the Complaint purports to state a cause of acti on under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patent

asserted against Microsoft in the Complaint. Microsoft denies any and all remaining allegations of paragraph 9 of the Complaint.

10. Microsoft denies, or lacks information and belief sufficient to admit or deny as to InterTrust's claim as to any and all allegations of paragraph 10 of the Complaint.

11. Microsoft denies any and all allegations of paragraph 11 of the Complaint.

12. Microsoft denies any and all allegations of paragraph 12 of the Complaint.

13. Microsoft denies any and all allegations of paragraph 13 of the Complaint.

14. Microsoft denies any and all allegations of paragraph 14 of the Complaint.

AFFIRMATIVE AND OTHER DEFENSES

Further answering the Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patent

15. Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,157,721 ("the '721 Patent"), and is not liable for infringement thereof.

16. Any and all Microsoft products or actions that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '721 Patent.

Second Defense: Invalidity of the Asserted Patent

17. On information and belief, the '721 Patent is invalid for failing to comply with the provisions of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailability of Relief

18. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 271(b) and is not entitled to any alleged damages prior to providing any actual notice to Microsoft of the '721 Patent.

Fourth Defense: Unavailabiltv of Relief

19. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to providing any actual notice to Microsoft of the '721 Patent, and any alleged infringement thereof.

Fifth Defense: Unavailabilitv of Relief

20. On information and belief, Plaintiff has failed to plead and meet the requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any damages.

Sixth Defense: Prosecution Historv Estoppel

21. Plaintiff's alleged cause of action for patent infringement is barred under the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '721 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

22. Plaintiff (and its predecessors in interest) has dedicated to the public, and abandoned, all methods, apparatus, and products (a) disclosed in U.S. Patent No. 5,940,504 and not literally claimed therein, (b) disclosed in U.S. Patent No. 5,892,900 and not literally claimed therein, (c) disclosed in U.S. Patent No. 5,917,912 and not literally claimed therein, (d) disclosed in U.S. Patent No. 5,920,861 and not literally claimed therein, (e) disclosed in U.S. Patent No. 5,982,891 and not literally claimed therein, (f) disclosed in the '721 Patent and not literally claimed therein, (g) disclosed in U.S. Patent No. 6,185,683 B1 and not literally claimed therein, and/or (h) disclosed in U.S. Patent No. 6,253,193 B1 and not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture Bv/For United States Government

23. To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

24. To the extent that Plaintiff's allegation of infringement is premised on the alleged

use, sale, or offer for sale of a product that was manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft to or by a licensee of InterTrust, such allegation is barred pursuant to license.

Tenth Defense: Acquiescence

25. Plaintiff has acquiesced in at least those acts of Microsoft that are alleged to infringe the '721 Patent.

Eleventh Defense: Laches

26. Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

27. The '721 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Count III of Microsoft's Counterclaims, set forth below.

Thirteenth Defense: Unenforceability

28. The claims of the '721 Patent are unenforceable due to unclean hands, inequitable conduct and misuse and illegal extension of the patent right, including those acts and failures to act set forth in Count IV of Microsoft's Counterclaims, set forth below.

COUNTERCLAIMS
COUNT I – DECLARATORY JUDGMENT OF NONINFRINGEMENT

1. This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, *et seq*. This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

2. Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

3. On information and belief, Plaintiff /Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

4. InterTrust purports to be the owner of U.S. Patent No. 6,157,721 ("the '721 Patent").

5. InterTrust alleges that Microsoft has infringed the '721 Patent.

6. InterTrust issued a press release on February 7, 2002. The press release stated that InterTrust had filed a lawsuit against Microsoft for patent infringement. The press release specificed that InterTrust "alleges infringement by Microsoft's 'Plug and Play' Driver Certification Program."

7. Microsoft's certification of hardware drivers has not infringed, either directly or indirectly, any claim of the '721 Patent, and Microsoft is not liable for infringement thereof.

8. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the infringement or noninfringement of the '721 Patent.

COUNT II – DECLARATORY JUDGMENT OF INVALIDITY OF THE '721 PATENT

9. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

10. The '721 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

11. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are valid or invalid.

COUNT III – DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '721 PATENT

12. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated herein.

13. Claims 1-43 of the '721 Patent application (SN 08/689,754), and claims 1-41 of the '721 Patent, were not and are not entitled to the benefit of any application filing date prior to August 12, 1996, under 35 U.S.C. § 120 or otherwise.

14. United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8, 1999, from a continuation of an application filed on February 13, 1995.

15. The '987 Patent is prior art to claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754).

16. The '987 Patent is prior art to claims 1-41 of the '721 Patent under 35 U.S.C. § 102(e).

17. The '987 Patent was material to the patentability of claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754).

18. One or more of the '721 Patent applicants knew, while the '721 Patent application (SN 08/689,754) was pending, of the '987 Patent.

19. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '721 Patent application (SN 08/689,754) knew, while that application was pending, of the '987 Patent.

20. The applicants for the '721 Patent did not cite the '987 Patent to the Patent Office as prior art to any of claims 1-43 of the '721 Patent application (SN 08/689,754).

21. The applicants for the '721 Patent did not cite to the Patent Office as prior art to any of claims 1-43 of the '721 Patent application (SN 08/689,754) any reference having the same or substantially the same disclosure as the '987 Patent.

22. The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '721 Patent application (SN 08/689,754).

23. On information and belief, one or more of the '721 Patent applicants believed, while the '721 Patent application (SN 08/689,754) was pending, that the '987 Patent was material to the patentability of one or more of claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

24. The '721 Patent is unenforceable due to the inequitable conduct of the '721 Patent applicants and/or agents before the Patent and Trademark Office in connection with the '721 Patent application (SN 08/689,754).

25. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are enforceable.

COUNT IV – DECLARATORY JUDGMENT OF UNENFORCEABILITY

26. Microsoft repeats and realleges paragraphs 1-5 and 12-24 of its Counterclaims, as if fully restated herein.

27. In prosecuting, marketing, and enforcing various related patents, including the '721 Patent, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents. For example, InterTrust has accused non-infringing products of infringement, has buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the particular claims in issue, and has buried the Examiners with hundreds or thousands of pages of redundant, verbose, unclear text, effectively prohibiting a real comparison of the alleged "invention" versus the prior art. This pattern of intentional conduct constitutes an abuse of the patent system, unclean hands, misuse and illegal extension of the patent right, rendering the '721 Patent unenforceable, as well as invalid under Section 112.

28. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are enforceable.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A. The Court enter judgment against InterTrust, and dismiss with prejudice, any and all claims of the Complaint;

B. The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '721 Patent;

C. The Court enter judgment declaring that the '721 Patent is invalid;

D. The Court enter judgment declaring that the '721 Patent is unenforceable due to inequitable conduct;

E. The Court enter judgment declaring that the '721 Patent is unenforceable due to abuse of the patent system, unclean hands, and misuse and illegal extension of the patent right;

F. The Court award attorney fees against InterTrust pursuant to the provisions of 35 U.S.C § 285;

G. The Court award to Microsoft pre-judgment interest and the costs of this actions;

H. The Court award to Microsoft its reasonable costs and attorneys' fees; and

I. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

Dated: April 12, 2002

By: ________________________
WILLIAM L. ANTHONY, JR.
ERIC L. WESENBERG
HEIDI L. KEEFE
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

STEVEN R. ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant/Counterclaimant
MICROSOFT CORPORATION

Of Counsel:
T. Andrew Culbert, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Telephone: (425) 936-6921

DECLARATION OF SERVICE VIA ELECTRONIC MAIL AND U.S. MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 1000 Marsh Road, Menlo Park, California 94025.

On April 12, 2002, I served:

MICROSOFT CORPORATION'S FIRST AMENDED ANSWER AND COUNTERCLAIMS

By transmitting a copy of the above-listed document(s) in PDF form via electronic mail **Michael H. Page at mhp@kvn.com, Christopher P. Isaac at chris.isaac@finnegan.com, Stephen E. Taylor at staylor@tcolaw.com and James E. Geringer at james.geringer@klarquist.com** and also by placing true and correct copies of the above documents in an envelope addressed to:

John W. Keker, Esq.
Michael H. Page, Esq.
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111
Tel. No. 415-391-5400
Fax No. 415-397-7188
Email: jwk@kvn.com
Email: mhp@kvn.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Christopher P. Isaac, Esq.
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER LLP
1300 I. Street, N.W.
Washington, DC 20005-3314
Tel. No. 202-408-4000
Fax No. 202-408-4400
Email: chris.isaac@finnegan.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Stephen E. Taylor, Esq.
TAYLOR & CO. LAW OFFICES
1050 Marina Village Parkway, Suite 101
Alameda, CA 94501
Tel. No. 510-865-9401
Fax No. 510-865-9408
Email: staylor@tcolaw.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

John D. Vandenberg, Esq.
James E. Geringer, Esq.
KLARQUIST, SPARKMAN, LLP
One World Trade Center
121 S. W. Salmon Street, Suite 1600
Portland, Oregon 97204
Tel. No: 503-226-7391
Fax No: 503-228-9446
Email: john.vandenberg@klarquist.com
Email: james.geringer@klarquist.com

Attorneys for Defendant and
Counterclaimant, MICROSOFT
CORPORATION

///

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Menlo Park, California.

Executed on April 12, 2002 at Menlo Park, California.

I declare under penalty of perjury that the foregoing is true and correct.

____
Print Name

____
Signature

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES
CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a
Washington corporation,

Defendant.

MICROSOFT CORPORATION, a
Washington corporation,

Counterclaimant,

v.

INTERTRUST TECHNOLOGIES
CORPORATION, a Delaware corporation,

Counter Claim-Defendant.

CASE NO. C02-0647 SBA
Consolidated with C01-1640 SBA

MICROSOFT'S INITIAL DISCLOSURES PURSUANT TO FED. R. CIV. P. 26(a)(1) ('721 Patent)

Pursuant to Fed. R. Civ. P. 26(a), Microsoft Corporation ("Microsoft") makes the following initial disclosures. The initial disclosures are based on information now reasonably available and Microsoft's current understanding of the claims and defenses in this case. Microsoft is not providing documents or information not reasonably available at this time. Microsoft reserves the right to object to discovery into any listed subject matter. Microsoft reserves the right to supplement this initial disclosure pursuant to Fed. R. Civ. P. 26(e).

A. Witnesses

Microsoft identifies the following potential witnesses who, based on information and belief, are likely to have discoverable information relevant to claims and defenses in the action originally titled C02-0647 EDL (since reassigned and consolidated with C01-1640 SBA), along with the possible subjects of their testimony.

Microsoft incorporates by reference the identity of any individual identified in the Patent Office file histories of the patents-in-suit, including U.S. Patent No. 6,157,721 ("the '721 Patent"), or involved in the prosecution of any patent-in-suit as being a potential source of discoverable information relevant to the '721 Patent, including but not limited to the named inventors, the prosecuting attorneys, and the U.S. Patent Office Examiners.

The individuals listed below may have discoverable information relevant to claims and defenses in this case. The identified individuals may also have information relevant to other subject matter areas that may be revealed upon further investigation of the matters at issue. There may be Microsoft employees, the specific identities of whom are not presently known, who are likely to have discoverable information relevant to claims and defenses in this action. In addition, there may be other persons and entities known to Microsoft who have discoverable information relevant to these subject matters, including Independent Software Vendors, Microsoft certified solution providers, Microsoft certified trainers, application developers, IT professionals, etc. Microsoft reserves the right to identify additional individuals who may have discoverable information relevant to any product that may be accused as infringing the '721 Patent, should InterTrust identify any such product. Microsoft employees may be contacted in this action only through Microsoft's counsel.

Microsoft incorporates its disclosure of November 26, 2001 regarding individuals employees who have information concerning pre-suit business negotiations between Microsoft and InterTrust, and licensing of patents-in-suit, and information relevant to prior art to the asserted InterTrust patents. On information and belief, at least the following additional individuals have information relevant to prior art to the '721 Patent: Dorothy Denning, George Davida, Yvo Desmedt, Whitfield Diffie, Robert S. Gray, T.E. Gray, Martin Hellman, Richard J. Linn, Brian Matt, Ralph Merkle, M.M. Pozzo, Dan Wallach, and anyone or anyone else familiar with the use or proposed use prior to the '721 Patent's filing date of cryptographic signatures and/or other "security" in Java, Telescript, Tcl, Verisign or Authenticode. Microsoft further incorporates by reference the identity of the authors, named inventors, and other individuals reflected or referenced in the publications and patents that are listed in the patents-in-suit and file histories or in Microsoft's Notice of Deposition of InterTrust Pursuant to Fed. R. Civ. P. 30(b)(6). Additional individuals potentially knowledgeable about prior art that may be relevant to the '721 Patent are reflected in documents produced by Microsoft in this matter. Microsoft also incorporates by reference any individuals disclosed by InterTrust who are likely to have discoverable information relevant to disputed facts alleged in the pleadings. Microsoft reserves the right to supplement the identity of possessors of material information pursuant to the Federal Rules of Civil Procedure and the Local Rules.

B. Documents

Microsoft has already produced or is producing for inspection and/or copying nonprivileged documents in its possession, custody or control which it may use to support a claim or defense relevant to the disputed facts alleged with particularity in the pleadings. Microsoft objects to the production of attorney-client communications, attorney work product or other information protected from discovery. Documents withheld on grounds of attorney-client privilege and/or work product immunity will be identified on a privilege log to be provided at a time mutually agreeable to the parties or ordered by the Court. Work product and confidential communications seeking or providing legal advice, or pursuant to the seeking or providing of legal advice, between Microsoft (or its agents) and attorneys (or their agents) representing

Microsoft in connection with such representation produced after October 17, 1994, are also withheld, without particular identification, as subject to the attorney-client privilege and/or work product immunity. This categorical identification of these documents is considered to satisfy any identification requirements necessary to properly assert privilege for these documents. See Advisory Committee notes to 1993 Amendments to Fed. R. Civ. P. 26(b).

C. Computation of Damages

As to the infringement claim(s) asserted by InterTrust, Microsoft asserts that it has no liability in relation to the '721 Patent (or any other InterTrust patent asserted in this action), and as a result there is no applicable computation of damages therefor. Microsoft reserves the right to recover attorneys fees and costs to the extent permitted by law. Microsoft anticipates that its response to any computation of alleged damages by InterTrust pertaining to the '721 Patent, and supporting documents and other evidentiary materials, will be made available during the course of discovery, including expert discovery, in this action.

D. Insurance Agreements

Microsoft is not aware of any insurance agreement relevant to this action under Fed. R. Civ. P. 26(a)(1)(D).

Dated: June 5, 2002

By: ______________________________
WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street

Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
MICROSOFT CORPORATION

DECLARATION OF SERVICE BY E-MAIL AND FIRST-CLASS MAIL

On June 5, 2001, I served:

MICROSOFT'S INITIAL DISCLOSURES
PURSUANT TO FED. R. CIV. P. 26(a)(1) ('721 Patent)

by e-mail delivery, and by placing a true copy of this paper in separate envelopes, first-class postage pre-paid, in the U.S. mail addressed to:

Michael H. Page, Esq. Keker & Van Nest, LLP 710 Sansome Street San Francisco, CA 94111 Phone.: 415-391-5400 Fax: 415-397-7188 E-mail: mhp@kvn.com	Stephen E. Taylor, Esq. Taylor & Co. Law Offices 1050 Marina Village Parkway Suite 101 Alameda, CA 94501 Phone: 510-865-9401 Fax: 510-865-9408 E-mail: staylor@tcolaw.com
Steven H. Morrissett, Esq. Finnegan Henderson Farabow Garrett & Dunner Stanford Research Park 700 Hansen Way Palo Alto CA 94304-1016 steven.morrissett@finnegan.com	

James E. Geringer

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

INTERTRUST TECHNOLOGIES CORPORATION
DOUGLAS K. DERWIN - #111407
MARK SCADINA - #173103
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA **NOTICE OF APPLICATION AND APPLICATION FOR LEAVE TO AMEND COMPLAINT AND LOCAL RULE 3-1 DISCLOSURES; REQUEST FOR FURTHER CASE MANAGEMENT CONFERENCE**
AND COUNTER ACTION.	Judge: The Honorable Saundra B. Armstrong Date: October 22, 2002 Time: 1:00 p.m.

NOTICE OF APPLICATION

PLEASE TAKE NOTICE that plaintiff and counter-defendant InterTrust Technologies Corporation ("InterTrust") hereby applies, pursuant to Federal Rule of Civil Procedure 15(a), for leave to amend it Complaint in this action. InterTrust further applies, pursuant to Patent Local Rule 3-7, for leave to serve an amended Patent Local Rule 3-1 Disclosure of Asserted Claims and Preliminary Infringement Contentions. InterTrust also requests that the Court schedule a further Case Management Conference at its earliest convenience. This application is set for hearing on October 22, 2002, at 1:00 p.m. This application is based upon the following Memorandum of Points and Authorities, and upon the accompanying declarations of Michael H. Page and David P. Maher.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

InterTrust hereby applies for leave to amend its complaint, in the form attached hereto as Exhibit A, and to serve amended Patent Local Rule 3-1 disclosures, in order to include in this case significant additional infringements of its patents by Defendant Microsoft Corporation ("Microsoft"). Those additional infringements include Microsoft products and services introduced to the marketplace since the filing of InterTrust's initial complaint in this action, as well as infringements revealed as a result of discovery produced by Microsoft in the course of this litigation. If granted, leave to amend will add an additional four InterTrust patents (Nos. 5,915,019 ("the '019 patent"), 5,949,876 ("the '876 patent"), 6,112,181 ("the '181 patent") and 6,389,402 B1 ("the '402 patent")) to the seven patents already in suit.

Leave to amend should be granted, as a matter of course, for numerous reasons:

- Although the proposed amendment adds additional patents, the patents are closely related to those already in suit; all but one is a continuation or continuation-in-part from the same parent application as the current patents-in-suit, sharing substantially the same specification.

- The additional patents do not add any inventors to the suit, and Microsoft has not yet deposed any of the inventors.

- All documents related to the invention and reduction to practice of the four additional patents have already been produced in response to previous Microsoft discovery requests, and thus no additional discovery from InterTrust will be required.

- In advance of this motion and contemporaneous with claim charts for the existing patents-in-suit, InterTrust provided Microsoft with complete draft claim charts for the four additional patents (claim charts that under the Patent Local Rules would not have been due for months after filing), thus obviating any delay caused by amendment.

- In the absence of leave to amend, InterTrust would be required (and entitled) to file the new allegations of infringement as a separate case, which in due course

> either (a) would be related to and consolidated with the existing suit anyway, after unnecessary delay and motion practice, or (b) would proceed separately, requiring two Markman hearings construing multiple identical terms and two trials, both raising the distinct possibility of conflicting rulings.

Basic principles of judicial economy and established rules of procedure dictate that leave to amend be granted in such circumstances. InterTrust, in advance of filing this application, served upon Microsoft amended claim charts for the existing patents-in-suit and complete claim charts for the four additional patents, and asked that Microsoft stipulate to leave to amend. See Declaration of Michael H. Page ("Page Decl."), ¶¶ 5-9 & Exhs.C,D. Microsoft declined to stipulate, necessitating this application.[1] Id., ¶ 6-9 & Exhs. E, G.

II. STATEMENT OF FACTS

This action has been pending for some fifteen months. As one would expect in any litigation concerning "cutting edge" technology, the world has not stood still while this case has been pending. Microsoft has continued to release new versions of its software, and has unveiled numerous new products, services, and initiatives. Chief among those initiatives has been Microsoft's ".NET" initiative, Microsoft's next generation technology platform. Since this lawsuit was filed, Microsoft has rolled out myriad aspects of .NET, and has begun publishing sufficient information about its .NET architecture to enable InterTrust to identify numerous additional infringements of its patents. As set forth in the accompanying Declaration of David P. Maher, InterTrust's Chief Technical Officer (hereafter, "Maher Decl."), significant technical source material used to identify those infringements was not available until late 2001 or 2002. Maher Decl., ¶5.

In addition, since this lawsuit was filed, Microsoft has shipped new versions of its operating system (Windows XP), has unveiled the Xbox gaming system, has introduced or updated technologies such as Windows CE for Automotive, Microsoft's driver signing

[1] In addition to adding four new patents, InterTrust's proposed amended complaint includes U.S. Patent No. 6,157,721, which is currently asserted in a separate but related and consolidated action, No. C 02 0647 SBA. The amended complaint makes no changes in the allegations related to that patent, and incorporates it only in order to fully consolidate the pending actions under a single case number. Upon filing of the Fourth Amended Complaint, the consolidated case could then be dismissed as moot.

technology, and its Media Player application, and has implemented numerous new technologies to allow secure computing across multiple distributed machines. Maher Decl. ¶¶ 6, 7. In each instance, and others, Microsoft has only later published technical disclosures and other information concerning these infringing technologies. Only as technical disclosures and publications concerning these new products and services have become available, InterTrust has been able to identify additional infringements of its patents. An extensive list of these sources, published or released in late 2001 and 2002, is contained in the Declaration of David P. Maher.

Similarly, time has not stood still at InterTrust. Pending patent applications have resulted in additional patents being issued to InterTrust, including the '402 patent, issued in May of this year. In its proposed amended complaint, InterTrust alleges infringement of this new patent. Moreover, analysis of material produced by Microsoft in discovery has revealed additional infringed claims from the patents-in-suit.[2]

As a result, it is again necessary for InterTrust to amend both its complaint and its Local Rule 3-1 disclosures, in order to assert all currently known claims in a single action. Those claims include four additional patents. Three of the four additional patents (the '019, 876, and '402 patents) are continuations or divisionals of the same original patent application from which five of the seven patents-in-suit arose. As a result, they share the same inventorship, and substantially the same specification, as the patents already in suit. Thus, there is little or no additional discovery that needs be taken concerning the inventorship of these additional patents: all documents concerning that invention and reduction to practice have already been produced, as well as file histories and draft claim charts. And as Microsoft has not yet deposed any of the inventors or any of the prosecuting attorneys, adding these patents will not result in duplicative discovery. Indeed, Microsoft has to date taken only one deposition of a third party, which will not need to be reconvened as a result of the proposed amendments. The fourth additional patent

[2] Just as with the additional patents, InterTrust on April 30 and again on June 21 served amended claim charts detailing additional claims from the patents-in-suit. Page Decl. ¶ 6 & Exh C. Microsoft has taken the position that InterTrust must seek leave of Court to serve those amended claim charts. Id., Exhs.E, G. Accordingly, InterTrust asks that the Court, in granting leave to amend and setting a revised schedule, also grant leave to serve those supplemental claim charts.. See Part II (B), infra.

(the '181 patent), although it is not a continuation of other patents-in-suit, springs from the same research efforts at InterTrust, and shares inventorship with the existing patents-in-suit. And again, all documents related to that patent have already been produced, as have file histories and draft claim charts.

Similarly, adding the four additional patents will have only limited impact on the conduct of this case under the Local Patent Rules. InterTrust has already produced claim charts for all eleven patents, and Microsoft has not yet served its Patent Local Rule 3-2 invalidity contentions. Although Microsoft will of course be required to present invalidity contentions for eleven patents rather than seven, and the parties and the Court will have to conduct claim construction hearings on eleven patents, the significant overlap of both subject matter and specifications (and thus the significant overlap of terms to be construed) means that Markman proceedings for all eleven patents will be at most only incrementally more complex than proceedings on the existing seven patents: with few if any exceptions, the terms to be construed extend across the entire body of patents. Indeed, given the close relationship between the various InterTrust patents, it would be wildly inefficient to litigate the newer infringements in a separate case, requiring two separate Markman hearings in two separate matters, with near-complete overlap of the terms to be construed.

III. ARGUMENT

A. LEAVE TO AMEND THE COMPLAINT SHOULD BE GRANTED

Federal Rule of Civil Procedure 15(a) provides that leave to amend a complaint "shall be freely given when justice so requires." See also Bowles v. Reade, 198 F.3d 752, 757 (9th Cir. 1999) (noting that the federal rules evidence a "strong policy permitting amendment"). "Rule 15's policy of favoring amendments to pleadings should be applied with extreme liberality." DCD Programs, Ltd. v. Leighton, 833 F.2d 183, 186 (9th Cir. 1987). The Ninth Circuit has noted that, when determining whether to grant leave to amend, a court must evaluate five factors: (1) bad faith by the moving party; (2) undue prejudice to the opposing party; (3) undue delay by the moving party; (4) futility of the amendment; and (5) whether the moving party has previously

///

amended its complaint. Id. at 186 & n.3. The party opposing amendment bears the burden of showing prejudice. Id. at 187.

Each of these factors militates for leave to amend. There can be no question that InterTrust has acted in good faith: InterTrust could not have included in its initial complaint infringement allegations concerning products and services that had not yet been released (or for which Microsoft had not yet released technical information), or based on patents that had not yet issued. Moreover, InterTrust advised Microsoft many months ago that it expected to add additional infringement allegations based on new information. That issue was discussed at length in the course of preparing the April 1, 2002 Case Management Conference Statement, which expressly sets forth both InterTrust's intention to add additional claims at the agreed-upon time of serving additional Patent Local Rule 3-1 disclosures and the parties' respective positions concerning what effect those additional claims would have on the proposed litigation schedule. Page Decl., ¶¶ 2-5 & Exhs. A & B at 11.[3]

Similarly, leave to amend will not cause any undue prejudice to Microsoft. As noted above, Microsoft has not conducted any depositions of inventors or prosecuting attorneys, so no discovery will need to be repeated. Neither are there any significant rulings that need be revisited, as no claim construction, infringement, or validity issues have yet been decided. Other than document discovery (which, as noted above, has on the InterTrust side covered the proposed additional patents as well as those in suit), this case is despite its age in the early stages of litigation. Admittedly, the allegations of infringement against additional Microsoft products and services expands the scope of the case—and the scope of discovery that must be provided by Microsoft—beyond that of the existing claims. But that is a function of Microsoft's vastly expanded infringement of InterTrust's patents, not of the proposed amendment, and those claims will be brought against Microsoft regardless whether leave is granted to amend this complaint. If

[3] Due in large part to Microsoft's decision to file its ill-fated summary judgment motion, which it later withdrew, that Case Management Conference was first rescheduled to coincide with the hearing of that motion, and then cancelled along with the withdrawn motion. As a result, the parties have been proceeding on a proposed litigation schedule that has never been approved by the Court. InterTrust respectfully urges that a Case Management Conference be held at the Court's earliest convenience.

anything, bringing those additional claims into this case will streamline the overall course of litigation between these parties.

Nor can there be a claim that InterTrust has unduly delayed bringing these additional claims. InterTrust has diligently researched new Microsoft products and services as they have been released, and as technical details of their operation have become available. InterTrust has at all times advised Microsoft timely of additional claims, and has even taken the step of providing Microsoft with Local Rule 3-1 claim charts in advance of filing its amended complaint—claim charts that would not actually be due for many months. InterTrust has also diligently brought additional claims into the existing complaint in this action, rather than hold claims back.[4]

And finally, there can be no question of futility here: this is not a case where leave to amend is sought in response to a prior dismissal, and thus where the Court can assess whether any proposed amendment could cure a previously-adjudicated defect. Rather, these are new claims, occasioned by additional infringing acts by Microsoft.

Conversely, refusal of leave to amend would unduly prejudice InterTrust. Absent leave to amend, InterTrust will be forced to file a separate action, which will begin an entirely new one- to two-year process leading to a largely redundant Markman proceeding. As a result, Microsoft will be able to avoid trial of its current technology almost indefinitely: as that second filing wends its way to trial, Microsoft will undoubtedly continue to release new versions of its software, and continue to resist amendment to encompass its current products. Microsoft will undoubtedly argue that there must be some point at which the pleadings must be fixed, and they are correct in principle. But that time is not now, while discovery is still open, no substantive depositions have been conducted by Microsoft, no substantive rulings have been made, and no invalidity or claims construction positions have been taken. At this early stage, InterTrust submits that the proper and judicially efficient course is to amend the current complaint to

///

[4] As a result, this is InterTrust's Fourth Amended Complaint, but that should not weigh against InterTrust's amendment here: rather, it is evidence of InterTrust's diligent attempts to avoid

encompass all known claims, so that validity and claims construction proceedings can be conducted once rather than multiple times.

B. LEAVE TO SERVE AMENDED PATENT LOCAL RULE 3-1 DISCLOSURES SHOULD BE GRANTED

The Court should also grant leave for InterTrust to serve its amended Patent Local Rule 3-1 disclosures—amended disclosures that have already been served upon Microsoft on June 21, 2002. Patent Local Rule 3-7 provides that preliminary or final infringement contentions may be amended or modified upon a showing of good cause. There can be no dispute that good cause exists for InterTrust to amend its claim charts in this case. The proposed amendments do not change previous infringement positions in order to avoid the effect of prior rulings, as was the case in Atmel Corp. v. Information Storage Devices, 1998 U.S. Dist. LEXIS 17564 (1998) (rejecting attempt to amend claim charts after Markman ruling and with summary judgment motions pending). Rather, they add additional claims of infringement based upon new Microsoft products and services, and based upon documents produced by Microsoft since service of InterTrust's preliminary claims charts. As set forth above and in the Declaration of David P. Maher, the proposed amendments are based in large part on information that was not made available by Microsoft until late last year and this year.

Neither can there be any possible prejudice to Microsoft as a result of the amended claims charts. Although InterTrust's prior claim charts were served in November, 2001, nothing of substantive effect has occurred since. Microsoft has not taken any positions in reliance on the prior claim charts: in fact, Microsoft has not yet even served its Patent Local Rule 3-3 Preliminary Invalidity Contentions. Under the Patent Local Rules, those disclosures are the next step after Rule 3-1 claim charts, and are supposed to be served 45 days after Rule 3-1 disclosures. Microsoft can hardly claim to be prejudiced by amendment of InterTrust's claim charts when it has not even proceeded to the next step in the process. Neither have there been any substantive decisions by the Court in the interim.

///

undue delay and prejudice.

Conversely, denial of leave to serve amended claim charts would severely prejudice InterTrust. Denial of leave would mean that Microsoft could avoid liability for significant portions of its ongoing patent infringement simply by releasing new products and services after service of InterTrust's initial disclosures. Unless leave is granted to bring new and newly-discovered infringements into this case, InterTrust would be required to file a separate lawsuit, asserting the same patents against the same defendant, every time Microsoft shipped another infringing product. And, assuming such seriatim complaints were required, Microsoft would upon resolution of the first case surely argue that subsequent cases, filed during the pendency of the first suit, were barred either by res judicata or as impermissibly split causes of action. And of course—as noted above—such seriatim cases would almost certainly be related and consolidated with this case in any event. Where—as here—no prejudice flows from amending the existing claim charts at this early stage, the more logical course is to simply allow the new claims to be amended into the pending litigation. Any other course would be a waste of judicial resources.

IV. CONCLUSION

For the foregoing reasons, InterTrust respectfully requests that the Court (1) grant leave to file InterTrust's Fourth Amended Complaint, (2) grant InterTrust leave to serve amended Patent Local Rule 3-1 disclosures, (3) order the consolidated case No. C 02 0647 SBA dismissed as moot, and (4) set a further Case Management Conference at the Court's earliest convenience for the purpose of setting a revised Case Management schedule.

Respectfully submitted.

Dated: July 30, 2002

KEKER & VAN NEST, LLP

By: ______________________
MICHAEL H. PAGE
Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

INTERTRUST TECHNOLOGIES CORPORATION
DOUGLAS K. DERWIN - #111407
MARK SCADINA - #173103
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA **[PROPOSED] FOURTH AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 6,185,683 B1; 6,253,193 B1; 5,920,861; 5,892,900; 5,982,891; 5,917,912; 6,157,721; 5,915,019; 5,949,876; 6,112,181; AND 6,389,402 B1.** **DEMAND FOR JURY TRIAL**
AND COUNTER ACTION.	

Plaintiff INTERTRUST TECHNOLOGIES CORPORATION (hereafter "InterTrust") hereby complains of Defendant MICROSOFT CORPORATION (hereafter "Microsoft"), and alleges as follows:

JURISDICTION AND VENUE

1. This action for patent infringement arises under the patent laws of the United

States, Title 35, United States Code, more particularly 35 U.S.C. §§ 271 and 281.

2. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(c) and 1400(b).

THE PARTIES

4. Plaintiff InterTrust is a Delaware corporation with its principal place of business at 4750 Patrick Henry Drive, Santa Clara, California.

5. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft is a Washington Corporation with its principal place of business at One Microsoft Way, Redmond, Washington.

6. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft does business in this judicial district and has committed and is continuing to commit acts of infringement in this judicial district.

7. InterTrust is the owner of United States Patent No. 6,185,683 B1, entitled "Trusted and secure techniques, systems and methods for item delivery and execution" ("the '683 patent"), duly and lawfully issued on February 6, 2001.

8. InterTrust is the owner of United States Patent No. 6,253,193 B1, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '193 patent"), duly and lawfully issued on June 26, 2001.

9. InterTrust is the owner of United States Patent No. 5,920,861, entitled "Techniques for defining, using and manipulating rights management data structures" ("the '861 patent"), duly and lawfully issued on July 6, 1999.

10. InterTrust is the owner of United States Patent No. 5,892,900, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '900 patent"), duly and lawfully issued on April 6, 1999.

11. InterTrust is the owner of United States Patent No. 5,982,891, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '891 patent"), duly and lawfully issued on November 9, 1999.

12. InterTrust is the owner of United States Patent No. 5,917,912 entitled "System

and methods for secure transaction management and electronic rights protection" ("the '912 patent"), duly and lawfully issued on June 29, 1999.

13. . InterTrust is the owner of United States Patent No. 6,157,721, entitled "Systems and methods using cryptography to protect secure computing environments" ("the '721 patent"), duly and lawfully issued on December 5, 2000.

14. InterTrust is the owner of United States Patent No. 5,915,019, entitled "Systems and methods for secure transaction management and electronic rights protection" (the '019 patent"), duly and lawfully issued on June 22, 1999.

15. InterTrust is the owner of United States Patent No. 5,949,876, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '876 patent"), duly and lawfully issued on September 7, 1999.

16. InterTrust is the owner of United States Patent No. 6,112,181, entitled "Systems and methods for matching, selecting, narrowcasting, and/or classifying based on rights management and/or other information" ("the '181 patent"), duly and lawfully issued on August 29, 2000.

17. InterTrust is the owner of United States Patent No. 6,389,402 B1, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '402 patent"), duly and lawfully issued on May 14, 2002.

FIRST CLAIM FOR RELIEF

18. InterTrust hereby incorporates by reference paragraphs 1-7 as if restated herein.

19. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

20. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '683 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '683 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under § 271(a) will continue unless enjoined by this Court.

21. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '683 patent under § 271(a), thereby inducing infringement of the '683 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under § 271(b) will continue unless enjoined by this Court.

22. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '683 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under § 271(c) will continue unless enjoined by this Court.

23. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '683 patent in the manner described above in paragraphs 20 through 22, and will continue to do so unless enjoined by this Court.

24. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SECOND CLAIM FOR RELIEF

25. InterTrust hereby incorporates by reference paragraphs 1-6 and 8 as if restated herein.

26. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

27. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '193 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '193 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under § 271(a) will continue unless enjoined by this Court.

28. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '193 patent under § 271(a), thereby inducing infringement of the '193 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under § 271(b) will continue unless enjoined by this Court.

29. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '193 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under § 271(c) will continue unless enjoined by this Court.

30. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '193 patent in the manner described above in paragraphs 27 through 29, and will continue to do so unless enjoined by this Court.

31. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of

infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

THIRD CLAIM FOR RELIEF

32. InterTrust hereby incorporates by reference paragraphs 1-6 and 9 as if restated herein.

33. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

34. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '861 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '861 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under § 271(a) will continue unless enjoined by this Court.

35. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '861 patent under § 271(a), thereby inducing infringement of the '861 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent under § 271(b) will continue unless enjoined by this Court.

36. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '861 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis

alleges, that Microsoft's infringement of the '861 patent under § 271(c) will continue unless enjoined by this Court.

37. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '861 patent in the manner described above in paragraphs 34 through 36, and will continue to do so unless enjoined by this Court.

38. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

FOURTH CLAIM FOR RELIEF

39. InterTrust hereby incorporates by reference paragraphs 1-6 and 10 as if restated herein.

40. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

41. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '900 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '900 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '900 patent under § 271(a) will continue unless enjoined by this Court.

42. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '900 patent under § 271(a), thereby inducing infringement of the '900 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '900 patent

under § 271(b) will continue unless enjoined by this Court.

43. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '900 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '900 patent under § 271(c) will continue unless enjoined by this Court.

44. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '900 patent in the manner described above in paragraphs 41 through 43, and will continue to do so unless enjoined by this Court.

45. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

FIFTH CLAIM FOR RELIEF

46. InterTrust hereby incorporates by reference paragraphs 1-6 and 11 as if restated herein.

47. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

48. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '891 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '891 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under § 271(a) will continue unless enjoined by this Court.

49. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '891 patent under § 271(a), thereby inducing infringement of the '891 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under § 271(b) will continue unless enjoined by this Court.

50. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '891 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under § 271(c) will continue unless enjoined by this Court.

51. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '891 patent in the manner described above in paragraphs 48 through 50, and will continue to do so unless enjoined by this Court.

52. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SIXTH CLAIM FOR RELIEF

53. InterTrust hereby incorporates by reference paragraphs 1-6 and 12 as if restated herein.

54. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

55. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '912 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '912 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '912 patent under § 271(a) will continue unless enjoined by this Court.

56. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '912 patent under § 271(a), thereby inducing infringement of the '912 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '912 patent under § 271(b) will continue unless enjoined by this Court.

57. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '912 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '912 patent under § 271(c) will continue unless enjoined by this Court.

58. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '912 patent in the manner described above in paragraphs 55 through 57, and will continue to do so unless enjoined by this Court.

59. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of

infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SEVENTH CLAIM FOR RELIEF

60. InterTrust hereby incorporates by reference paragraphs 1-6 and 13 as if restated herein.

61. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

62. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '721 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '721 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '721 patent under § 271(a) will continue unless enjoined by this Court.

63. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '721 patent under § 271(a), thereby inducing infringement of the '721 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '721 patent under § 271(b) will continue unless enjoined by this Court.

64. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '721 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis

alleges, that Microsoft's infringement of the '721 patent under § 271(c) will continue unless enjoined by this Court.

65. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '721 patent in the manner described above in paragraphs 62 through 64, and will continue to do so unless enjoined by this Court.

66. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

EIGHTH CLAIM FOR RELIEF

67. InterTrust hereby incorporates by reference paragraphs 1-6 and 14 as if restated herein.

68. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

69. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '019 patent under § 271(a), as identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '019 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '019 patent under § 271(a) will continue unless enjoined by this Court.

70. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '019 patent under § 271(a), thereby inducing infringement of the '019 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '019 patent under §

271(b) will continue unless enjoined by this Court.

71. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '019 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '019 patent under § 271(c) will continue unless enjoined by this Court.

72. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '019 patent in the manner described above in paragraphs 69 through 71, and will continue to do so unless enjoined by this Court.

73. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

NINTH CLAIM FOR RELIEF

74. InterTrust hereby incorporates by reference paragraphs 1-6 and 15 as if restated herein.

75. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

76. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '876 patent under § 271(a), as identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '876 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '876 patent under § 271(a) will continue unless enjoined by this Court.

77. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '876 patent under § 271(a), thereby inducing infringement of the '876 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '876 patent under § 271(b) will continue unless enjoined by this Court.

78. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '876 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '876 patent under § 271(c) will continue unless enjoined by this Court.

79. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '876 patent in the manner described above in paragraphs 76 through 78, and will continue to do so unless enjoined by this Court.

80. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

TENTH CLAIM FOR RELIEF

81. InterTrust hereby incorporates by reference paragraphs 1-6 and 16 as if restated herein.

82. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

83. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '181 patent under § 271(a), as identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '181 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '181 patent under § 271(a) will continue unless enjoined by this Court.

84. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '181 patent under § 271(a), thereby inducing infringement of the '181 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '181 patent under § 271(b) will continue unless enjoined by this Court.

85. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '181 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '181 patent under § 271(c) will continue unless enjoined by this Court.

86. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '181 patent in the manner described above in paragraphs 83 through 85, and will continue to do so unless enjoined by this Court.

87. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of

infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

ELEVENTH CLAIM FOR RELIEF

88. InterTrust hereby incorporates by reference paragraphs 1-6 and 17 as if restated herein.

89. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

90. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '402 patent under § 271(a), as identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '402 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '402 patent under § 271(a) will continue unless enjoined by this Court.

91. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '402 patent under § 271(a), thereby inducing infringement of the '402 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '402 patent under § 271(b) will continue unless enjoined by this Court.

92. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '402 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that

Microsoft's infringement of the '402 patent under § 271(c) will continue unless enjoined by this Court.

93. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '402 patent in the manner described above in paragraphs 90 through 92, and will continue to do so unless enjoined by this Court.

94. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, InterTrust prays for relief as follows:

A. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(a);

B. That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '683 patent under 35 U.S.C. § 271(a);

C. That Microsoft be adjudged to have contributorily infringed the '683 patent under 35 U.S.C. § 271(c);

D. That Microsoft be adjudged to have willfully infringed the '683 patent under 35 U.S.C. §§ 271(a), (b), and (c);

E. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '683 patent;

F. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(a);

G. That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '193 patent under 35 U.S.C. § 271(a);

///

H. That Microsoft be adjudged to have contributorily infringed the '193 patent under 35 U.S.C. § 271(c);

I. That Microsoft be adjudged to have willfully infringed the '193 patent under 35 U.S.C. §§ 271(a), (b), and (c);

J. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '193 patent;

K. That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. § 271(a);

L. That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '861 patent under 35 U.S.C. § 271(a);

M. That Microsoft be adjudged to have contributorily infringed the '861 patent under 35 U.S.C. § 271(c);

N. That Microsoft be adjudged to have willfully infringed the '861 patent under 35 U.S.C. §§ 271(a), (b), and (c);

O. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '861 patent;

P. That Microsoft be adjudged to have infringed the '900 patent under 35 U.S.C. § 271(a);

Q. That Microsoft be adjudged to have infringed the '900 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '900 patent under 35 U.S.C. § 271(a);

R. That Microsoft be adjudged to have contributorily infringed the '900 patent under 35 U.S.C. § 271(c);

S. That Microsoft be adjudged to have willfully infringed the '900 patent under 35 U.S.C. §§ 271(a), (b), and (c);

T. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '900 patent;

U. That Microsoft be adjudged to have infringed the '891 patent under 35 U.S.C. § 271(a);

V. That Microsoft be adjudged to have infringed the '891 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '891 patent under 35 U.S.C. § 271(a);

W. That Microsoft be adjudged to have contributorily infringed the '891 patent under 35 U.S.C. § 271(c);

X. That Microsoft be adjudged to have willfully infringed the '891 patent under 35 U.S.C. §§ 271(a), (b), and (c);

Y. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '891 patent;

Z. That Microsoft be adjudged to have infringed the '912 patent under 35 U.S.C. § 271(a);

AA. That Microsoft be adjudged to have infringed the '912 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '912 patent under 35 U.S.C. § 271(a);

BB. That Microsoft be adjudged to have contributorily infringed the '912 patent under 35 U.S.C. § 271(c);

CC. That Microsoft be adjudged to have willfully infringed the '912 patent under 35 U.S.C. §§ 271(a), (b), and (c);

DD. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '912 patent;

EE. That Microsoft be adjudged to have infringed the '721 patent under 35 U.S.C. § 271(a);

FF. That Microsoft be adjudged to have infringed the '721 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '721 patent under 35 U.S.C. § 271(a);

///

GG. That Microsoft be adjudged to have contributorily infringed the '721 patent under 35 U.S.C. § 271(c);

HH. That Microsoft be adjudged to have willfully infringed the '721 patent under 35 U.S.C. §§ 271(a), (b), and (c);

II. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '721 patent;

JJ. That Microsoft be adjudged to have infringed the '019 patent under 35 U.S.C. § 271(a);

KK. That Microsoft be adjudged to have infringed the '019 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '019 patent under 35 U.S.C. § 271(a);

LL. That Microsoft be adjudged to have contributorily infringed the '019 patent under 35 U.S.C. § 271(c);

MM. That Microsoft be adjudged to have willfully infringed the '019 patent under 35 U.S.C. §§ 271(a), (b), and (c);

NN. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '019 patent;

OO. That Microsoft be adjudged to have infringed the '876 patent under 35 U.S.C. § 271(a);

PP. That Microsoft be adjudged to have infringed the '876 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '876 patent under 35 U.S.C. § 271(a);

QQ. That Microsoft be adjudged to have contributorily infringed the '876 patent under 35 U.S.C. § 271(c);

RR. That Microsoft be adjudged to have willfully infringed the '876 patent under 35 U.S.C. §§ 271(a), (b), and (c);

///

///

SS. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '876 patent;

TT. That Microsoft be adjudged to have infringed the '181 patent under 35 U.S.C. § 271(a);

UU. That Microsoft be adjudged to have infringed the '181 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '181 patent under 35 U.S.C. § 271(a);

VV. That Microsoft be adjudged to have contributorily infringed the '181 patent under 35 U.S.C. § 271(c);

WW. That Microsoft be adjudged to have willfully infringed the '181 patent under 35 U.S.C. §§ 271(a), (b), and (c);

XX. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '181 patent;

YY. That Microsoft be adjudged to have infringed the '402 patent under 35 U.S.C. § 271(a);

ZZ. That Microsoft be adjudged to have infringed the '402 patent under 35 U.S.C. § 271(b) by inducing others to infringe directly the '402 patent under 35 U.S.C. § 271(a);

AAA. That Microsoft be adjudged to have contributorily infringed the '402 patent under 35 U.S.C. § 271(c);

BBB. That Microsoft be adjudged to have willfully infringed the '402 patent under 35 U.S.C. §§ 271(a), (b), and (c);

CCC. That Microsoft, its officers, agents, servants, employees and attorneys, and those persons in active concert or participation with them be preliminarily and permanently restrained and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '402 patent;

DDD. That this Court award damages to compensate InterTrust for Microsoft's infringement, as well as enhanced damages, pursuant to 35 U.S.C. § 284;

///

EEE. That this Court adjudge this case to be exceptional and award reasonable attorney's fees to InterTrust pursuant to 35 U.S.C. § 285;

FFF. That this Court assess pre-judgment and post-judgment interest and costs against Microsoft, and award such interest and costs to InterTrust, pursuant to 35 U.S.C. § 284; and

GGG. That InterTrust have such other and further relief as the Court may deem proper.

Dated: July __, 2002

KEKER & VAN NEST, LLP

By:____________________________
MICHAEL H. PAGE
Attorneys for Plaintiff and Counter Defendant
INTERTRUST TECHNOLOGIES CORPORATION

DEMAND FOR JURY TRIAL

Plaintiff InterTrust herby demands a trial by jury as to all issues triable by jury, specifically including, but not limited to, the issue of infringement of United States Patent Nos. 6,185,683 B1; 6,253,193 B1; 5,920,861; 5,892,900; 5,982,891; 5,917, 912; 6,157,721; 5,915,019; 5,949,876; 6,112,181; and 6,389,402 B1.

Dated: July ___, 2002

KEKER & VAN NEST, LLP

By: ____________________________
JOHN W. KEKER
Attorneys for Plaintiff and Counter Defendant
INTERTRUST TECHNOLOGIES CORPORATION

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE, State Bar No. 178960
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C01-1640 SBA Consolidated with C02-0647 SBA **MICROSOFT'S PRELIMINARY INVALIDITY CONTENTIONS REGARDING U.S. PATENTS 6,253,193 & 6,185,683 PURSUANT TO PLR 3-3, 3-4**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counterclaim-Defendant.	The Honorable Saundra B. Armstrong

InterTrust and its agents have engaged in a long pattern of misconduct that extends to and includes false and unsupported allegations of patent infringement. By way of example, the following information and attached charts illustrate that InterTrust has made invalid assertions of patent claim infringement under 35 U.S.C. §§ 102, 103 and 112 (limited to indefiniteness, non-enablement, and written description). Additional grounds for invalidity and unenforceability lie outside the scope of PLR 3-3 and are expressly reserved. Microsoft further reserves the unrestricted right to assert its defenses (and seek declaratory judgments) that the claims asserted by InterTrust are not infringed.

Microsoft has stated and preserves its objections and arguments as set forth in its motions on file and case management statements. Microsoft further notes and incorporates by reference its objections to InterTrust's improper attempts to modify its PLR 3-1 Statements without consent or leave of Court. Without limitation, Microsoft objects to InterTrust's refusal to provide a complete PLR 3-1 Statement for any of the InterTrust asserted patents, or to provide relevant information sought in discovery, including the identity of the alleged inventors of specific claims; conception or actual reduction to practice dates for specific claims; whether to its knowledge there has ever been any alleged embodiment(s) of asserted claims; and what if any specification support is alleged, including from any of the applications from which InterTrust claims priority. For example, InterTrust has failed to provide discovery regarding reduction to practice, including as set forth in Microsoft's motion to compel and the Court's rulings thereon. For another example, InterTrust has alleged that specific claims are entitled to rely on one or more earlier applications for priority, but has refused to state how. Microsoft expressly reserves the right to rely upon InterTrust's own activities, alone and in connection with others, as prior art, should InterTrust fully comply with relevant discovery. Microsoft further reserves the right to supplement this statement or otherwise further respond if InterTrust modifies its PLR 3-1 allegations (including but not limited to providing proper initial PLR 3-1 Statements), whether through motion or consent, or if InterTrust contends (or the Court rules) that any earlier or later priority date(s) may apply.

PLR 3-3(a, b)

This Statement responds to InterTrust's initial PLR 3-1 Statement regarding U.S. Patents 6,253,193 and 6,185,683 served on or about October 29, 2001. The identities of prior art references that anticipate claims as asserted in InterTrust's PLR 3-1 Statement or render them obvious are set forth below and in the attached PLR 3-3(c) charts. Please refer to the columns in the charts for further description of the references identified in abbreviated form below.

Asserted Claims	**References That Anticipate and/or Render Obvious**
'683 - 2, 28-29	Stefik, CUPID, CNI/IMA 94, Choudhury/Maxemchuk, Tygar/Yee, Neuman, Davies & Price, ATMs, Chaum, Telescript, NT, Bell-Lapadula, CUPID, Blaze, "secure" OODBs,Kerberos, Cox/Mori, Griswold, Cryptolopes, iOpener, iPower, Lampson
'193 - 1-4, 11, 15, 19	Stefik, Choudhury/Maxemchuk, Blaze, CNI/IMA 94, Hellman, CUPID, Chaum, Neuman

See also the cited art in the manner applied by the Examiners.

Each prior art reference identified herein and in the attached charts anticipates one or more asserted claims or renders them obvious. People having knowledge of this information prior to relevant priority dates include the authors/creators and recipients/users of each reference.

Entities making/receiving offers or information regarding products referenced herein include the following:

Item	**Date**	**exemplary entities making offer and/or information known**
NT, OLE, COM	1993 and continuing thru at least 2/12/95 and 2/24/97	Microsoft Corp.
Kerberos	before 1994 and continuing thru at least 2/12/95 and 2/24/97	MIT; B. Clifford Neuman
Strongbox, Dyad, Mach	before 1994 and continuing thru at least 1995	Carnegie Mellon Univ.; Doug Tygar; Bennet Yee, Rick Rashid
Stefik	at least by 1994 and continuing thru at least 2/12/95 and 2/24/97	Xerox; ContentGuard
CUPID	at least by 2/94 and continuing thru at least 2/12/95 and 2/24/97	See '683 chart
PolicyMaker	by 1996	AT&T
PersonaLink	at least prior to 2/12/95	AT&T
Telescript	at least by 1994	General Magic, AT&T, RSA
PGP	at least by 2/94 and continuing	Phil Zimmerman

1

	thru at least 2/12/95 and 2/24/97	
RSA software	at least before 2/12/95 and 2/24/97	RSA
iPower, iOpener	before 2/12/95	National Semiconductor
"secure" OODB systems (e.g., Orion, Itasca, Thor)	at least by 2/13/94 and continuing thru at least 2/12/95 and 2/24/97	MCC, Itasca, MIT (see '683 chart); IBEX
Cryptolope & InfoMarket	Before 2/12/95 and 2/24/97	IBM

From InterTrust's current document production, it appears that its employees' and consultants' activities, including offers for sale, public uses, derivations, and "inventions" (in the sense of Section 102(g)), and disclosures to Willis Ware, Drew Dean, and others not under any duty of confidentiality, constituted or created material and perhaps anticipatory prior art to many of the asserted claims, that was not cited to the Patent Office. Microsoft reserves the right to supplement this disclosure after Microsoft has had an opportunity to investigate this possible prior art in discovery.

Suggestions to combine & motivations to combine

Among the combinations obvious under § 103 are those set forth in each § 102 prior art reference cited herein, including D. Kahn, The Codebreakers (Macmillan 1967); L.D. Smith, Cryptography – the science of secret writing (Dover 1943, 1971); Bruce J. Walker and Ian F. Blake, Computer Security and Protection Structures (Dowden Hutchinson & Ross, Inc. 1977); D. Hsiao et al., Computer Security (Academic Press 1979); A. Konheim, Cryptography: A Primer (Wiley 1981); D. Denning, Cryptography and Data Security (Addison-Wesley 1982); Meyer, C.H., and Matyas, S.M., Cryptography - A New Dimension in Computer Data Security (Wiley 1982); Wood, Unix System Security (Hayden 1985); Elliott Irving Organick, The Multics System (MIT 5th ed. 1985); C.J. Date, An Introduction to Database Systems, 4th ed. (Addison-Wesley 1986); J. Cooper, Computers & Communications (McGraw Hill 1989); S. Muftic, Security Mechanisms for Computer Networks (Ellis Horwood 1989); Davies & Price, Security For Computer Networks (Wiley 1989); W. LaLonde and J. Pugh, Inside Smalltalk (Prentice Hall 1990); Computer Security (Time Life 1990); D. Russell et al., Computer Security Basics (O'Reilly 1991); S. Garfinkel, Practical Unix Security (O'Reilly 1991); CMU Computer Science: A 25th Anniversary Commemorative, R. Rashid, ed. (ACM Press 1991); D. Curry, Unix System

Security (Addison-Wesley 1992); Custer, Inside NT (Microsoft Press 1993); B. Schneier, Applied Cryptography (Wiley 1994) (also 2d ed. 1996); D. Dougherty, The Mosaic Handbook (O'Reilly 1994); Castano, Database Security (Addison-Wesley 1994); F. Cohen, Protection and Security on the Information Highway (Wiley 1995); A. Tanenbaum, Operating Systems, Design and Implementation (Prentice Hall 1987), Computer Networks, 2d ed. (Prentice Hall 1988), Modern Operating Systems (Prentice Hall 1992), and Distributed Operating Systems (Prentice Hall 1995); the work of Martin S. Olivier et al. cited in the attached '683 chart; the work of Morris Sloman, Jonathan Moffet, David Chaum, B. Clifford Neuman and Butler Lampson (see www.doc.ic.ac.uk/~mss/MSSPubs.html; www-users.cs.york.ac.uk/~jdm/jdmpubs.htm ; www.chaum.com/articles/list_of_articles.htm; http://www.isi.edu/people/bcn/publications.html; and research.microsoft.com/lampson/Publications.html); any single conference, meeting or proceedings, such as the January 1994 RSA Data Security Conference,[2] the April 1993 conference at Harvard University described in the deposition of Richard J. Linn, or Proceedings, Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project, vol. 1 no. 1 (Jan. 1994) ("CNI/IMA 94"). Additional obvious combinations include the combinations indicated in the asserted patents' file histories, related RFCs, work on a common project or product, and the combinations of any given author or named inventor's cumulative prior art work. For example, by "Stefik" this document refers to the referenced patents, acts and publications attributed in whole or part to Mark Stefik, taken individually or together. These make obvious, for example, that using methods in additive, iterative or other combinations could enhance overall "security," as would variation in individual steps or methods, such as encrypting, signing, or building files, using objects, and/or distributing in such a manner as to help do or protect things of value against unauthorized access, threats, or adverse effects. Adding or subtracting rights, or adding or repeating steps or functions (such as adding Kerberos to access control lists or capabilities, or watermarking binaries before and/or after encrypting any part of them), were simple variations of this. (See, e.g., Davies, Denning, Hellman, Neuman, Chaum, Linn, Blaze, Lampson, Tygar/Yee, Stefik, Choudhury/Maxemchuk, Moffett, Curry, Garfinkel/Spafford, Muftic, Carroll, Hsiao et al.). These further make obvious that one can automate any manual step

[2] See, e.g., Walker, Notes from RSA Data Security Conference, www.eff.org/Privacy/Crypto/Crypto_misc/rsa_conf.summary (Jan. 18, 1994); www.ddj.com/documents/s=1005/ddj9454d/9454d.htm, (Dr. Dobbs Journal).

in the exchange of encrypted information, or vice versa. For example, one or more steps of a communication or transfer could be "out of band".

The motivation for seeking "security," privacy, and integrity was widely recognized in the United States and elsewhere prior to February 13, 1994, and extends to any information or item of perceived value, including books, music, computer systems, and computer programs, as set forth in, e.g., Hellman, Stefik, Chaum, Choudhury, Date, Castano, Custer, Olivier, Russell, Muftic, Denning and/or Davies.[3] Additional motivations include the desire to meet or exceed any applicable laws or industry or government standards, such as the Orange Book, Computer Fraud and Abuse Act of 1986, Computer Security Act of 1989 PL100-35, High Performance Computing Act (HPCA) of 1991 (P.L. 102-194), and Title 17 U.S.C. § 101 et seq. (including, for example, § 1002). Industry standards include those for communication, such as X.509, TCP/IP, WWW, and WAIS, and those for encryption or transmission of encrypted information, e.g., DES, Triple DES, RSA, SSL, S/MIME, SHTTP, HTTPS, MD5, and PEM. Additional obviousness teachings to combine with such items or information include "security" levels, permissions, certificates, tickets, "secure" processors, "secure" storage, "smart" cards (including smart cards able to store data and perform computations such as encryption/decryption), tamper resistance techniques for hardware and software, physical "security," trusted time, authentication and authorization in trusted distributed systems, enabling software or features thereof to run only on particular machines, and treating binary information/data at varied levels of granularity. It was further obvious to combine any of these "security" features with any of the following software (or features thereof) and/or any of the following hardware (or features thereof) to provide any element or perform any step shown in the charts below:

> software: file and operating systems such as NT, NFS, Andrew, Netware, Mach, DT Mach, Multics, Unix, and in the Blaze and Tanenbaum and other references cited above; secure kernels; protocols, codes and systems such as WWW, SSL, SGML, hypertext, Oak, Telescript, OOP and other programming technologies or frameworks (e.g. Smalltalk, COM, OLE, Bento, Open Doc)[4]; object-oriented databases; watermarking; obfuscation (see, e.g., Choudhury at 15); swIPe; SNMP; auditing; on-line transaction and

[3] Regarding digital music, see also, e.g., J. Ratcliff, "Examining PC Audio," Dr. Dobb's Journal (March 1993).

[4] For example, it was obvious to use the prior art OOP technologies or frameworks to implement the systems described in e.g. Fischer, Linn, Stefik, Choudhury, Telescript, and object-oriented databases.

subscription-based services and billing; electronic payment; on-line banking, entertainment and commercial and interactive commerce; encryption and authentication (including e.g., "something you are, something you know, something you have"); hardware: physical security tools and devices; physically secure locations, physically "secure" products such as tamper resistant computers or other devices, "secure" processors, "secure" memory, "smart" cards, set-top boxes, portable devices, "secure" communication facilities.

See Stefik, CNI/IMA 94, Chaum, Tygar/Yee, Choudhury/Maxemchuk, Stefik, Denning, Davies, Moffett, Curry, Garfinkel/Spafford, Muftic, Carroll, Hsiao et al. and the other references cited above.

Each of these suggestions and motivations to combine apply to each of the references set forth in the attached charts.

PLR 3-3(c)

The attached charts identify, for each item of prior art, elements within the scope of InterTrust's October 29, 2001 PLR 3-1 allegations for the '683 and '193 patents. The structure, act or material for any such element if so construed is set forth in the references identified in the attached charts.[5]

PLR 3-3(d)

Each asserted claim is invalid as indefinite, for lack of enablement, and for lack of the written description required by statute. The present basis in each case is each applicable patent specification relied upon by InterTrust for the description required by paragraphs one and two of Section 112, and the prosecution histories of those applications and related applications as provided by law. Further basis may include, by way of example, any extrinsic evidence relevant to the construction of claim terms; InterTrust's own professed ignorance whether simple acts like playing music from a compact disc do not infringe asserted claims; and its difficulty, delay and/or inability to identify conception dates or actual reductions to practice of asserted claims.

[5] InterTrust has not identified any claim elements allegedly subject to § 112 ¶ 6 under PLR 3. Should InterTrust do so (and reserving any objection thereto), Microsoft reserves the right to respond to that issue.

<u>"Indefiniteness" of the Asserted InterTrust Patent Claims</u>[6]

In prosecuting, marketing, and enforcing the asserted InterTrust Patents, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents. For example, InterTrust has mechanically buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the claims, and has buried the Examiners with hundreds or thousands of pages of redundant, verbose, unclear text, effectively precluding a real comparison of the alleged "invention" versus the prior art, and accused non-infringing products of infringement. One result of InterTrust's approach is that the asserted patent claims are indefinite in myriad ways.

The asserted "claims" are unclear in scope and not nearly as precise as the subject matter allows. This indefiniteness arises from many causes, including:

- by use of terms that lacked any ordinary meaning in the art and are undefined in the specification;
- by use of terms that are used in the specification in a manner inconsistent with their ordinary meaning, but are not specifically defined in the specification;
- by a Section 112, ¶ 6 "means (or step) plus function" element having no specific structure in the application's written description clearly linked to that claim element (examples denoted below by underlining)[7];
- by such excessive disclaimers of specificity of a term that the term becomes meaningless;
- by inconsistent uses of a term within a single specification;
- by inconsistent uses of a term between a specification and something allegedly incorporated into that specification;
- by inconsistencies within the language of a given claim;

This lack of definiteness is exacerbated by InterTrust trying to apply these claims to the very different structures and techniques of (or that InterTrust mistakenly attributes to) Microsoft's accused software. Particularly in view of these untenable infringement accusations, the following bolded claim terms and phrases are indefinite under 35 U.S.C. § 112, ¶ 2. Microsoft reserves the

[6] For ease of reference only, the accompanying claim listings use the clause numbering and lettering used by InterTrust in its PLR 3-1 Statements.

[7] Other undefined, indefinite claim terms are so ambiguous that one or more possible constructions are purely functional such that the term, as so construed, is a Section 112, ¶ 6 limitation. Microsoft, therefore, reserves the right to identify additional claim limitations as

right to modify this listing, e.g., if and when InterTrust clarifies its infringement and claim construction positions.

<u>'193</u>

1) A method comprising:

a) **receiving** a digital **file including** music;

b) **storing** said digital **file in** a first **secure memory** of a first device;

c) **storing** information **associated with said digital file in a secure database** stored on said first device, said information **including** at least one **budget control** and at least one **copy control**, said at least one **budget control including a budget specifying the number of copies which can be made of said digital file**; and said at least one **copy control controlling the copies made of said digital file**;

d) **determining whether said digital file may be copied** and stored on a **second device based on at least said copy control;**

e) **if said copy control allows at least a portion of said digital file to be copied** and stored on a **second device,**

f) **copying at least a portion of** said digital **file**;

g) **transferring at least a portion** of said digital **file** to a **second device** including a **memory** and an **audio and/or video output**;

h) **storing** said digital **file in** said **memory** of said second device; and

i) including playing said music through **said audio output.**

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file including** music;	- "receiving … file" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "file," and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file." - "including" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or

Section 112, ¶ 6, limitations.

	excludes merely holding a reference.
b) **storing** said digital **file in** a first **secure memory** of a first device;	- see above - "storing … in" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - if "secure memory" is not at least limited to the disclosed internal RAM and/or ROM (directly addressable by a SPU processor instruction) located within the physically protected, "tamper-resistant"[8] SPU, the term "secure memory" would be indefinite. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure."
c) **storing** information **associated with said digital file in** a **secure database** stored on said first device,	- see above - if "associated with said digital file" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with said digital file" would be indefinite. - if "secure database" is not at least limited to the disclosed "secure database" (including its "secure

[8] Indefinite claim terms, such as "tamper-resistant," used in describing the indefiniteness of other claim terms, are used in their narrowest possible sense.

	database manager" and alleged access control "VDE" mechanisms), the term "secure database" would be indefinite.
said information **including** at least one **budget control**	- see above - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite. - "budget control" is not used in the specification and is indefinite.
and at least one **copy control,**	- see above - "copy control" is not used in the specification and is indefinite. For example, it is indefinite on whether "copy" is used as a verb or a noun. - "copy" is indefinite, e.g., on whether it encompasses or excludes something (or creating something) that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy."
said at least one **budget control including a budget specifying the number of copies which can be made of said digital file;**	- see above - "budget" is used inconsistently in the specification and is indefinite. For example, apparently it is used to refer sometimes to a "method," sometimes to a "component assembly," sometimes to a value, and sometimes to a UDE data structure. - "copies" is indefinite (see "copy" above) - if the phrase "specifying the number of copies which can be made of said digital file" is not at least limited to meaning the total global number of "copies" that ever will have been made of that "file" at any time, by any

	“user,” by any device, and for any length of persistence, it would be indefinite.
and said at least one **copy control controlling the copies made of said digital file**;	- see above - if “controlling” is not at least limited to use of the disclosed “component assembly,” “protected processing environment,” “object registration,” “secure container,” and other mechanisms of the purported “VDE” “invention” for allegedly individually ensuring that specific “controls” are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific “users,” the term “controlling” would be indefinite. - the phrase “controlling the copies made of said digital file” is indefinite, e.g., on whether it refers to “controlling” the process of “copying” the “file,” or “controlling” all resulting “copies” of the “file,” or both.
d) **determining whether said digital file may be copied and stored on a second device based on at least said copy control**;	- see above - “copied” is indefinite (see “copy” above) - “determining whether said digital file may be copied and stored on a second device” is indefinite, e.g., on whether this step determines whether the “file” may be “copied” on a second device, on whether one or more determinations are made. - “a second device” is indefinite, e.g., on whether it means “any” second device or a particular second device. - depending on the construction of other claim limitations, such as “at least one copy control controlling the copies made of said digital file” the phrase “based on at least said copy control” may be inconsistent with other limitations of this claim and thus may be indefinite.
e) **if said copy control allows at least a portion of said digital file**	- see above - “a portion of said digital file” is indefinite, e.g., on

to be copied and stored on **a second device,**	whether it encompasses or excludes matter that is merely referenced within the "file." - depending on the construction of other claim limitations, such as "based on at least said copy control," the phrase "if said copy control allows" may be inconsistent with other limitations of this claim and thus may be indefinite. - depending on the construction of other claim limitations, such as "at least one copy control controlling the copies made of said digital file," the phrase "if said copy control allows at least a portion of said digital file to be copied" may be inconsistent with other limitations of this claim, and thus may be indefinite.
f) **copying at least a portion of** said digital **file**;	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "copy control."
g) **transferring at least a portion** of said digital **file to a second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "copy control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or

	excludes a "portion" not "copied" in the preceding step. - "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the same particular second device referred to earlier in the claim (to the extent the claim earlier refers to a particular second device).
including a **memory**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
and an **audio and/or video output**;	- "audio and/or video output" is indefinite, e.g., it is inconsistent with the later claim recitation of "said audio output."
h) **storing** said digital **file in** said **memory** of said second device; and	- see above
i) including playing said music through **said audio output.**	- "said audio output" is indefinite, e.g., it is inconsistent with the earlier claim recitation of "audio and/or video output."

2) A method as in claim 1, further comprising:
a) at **a time substantially contemporaneous with** said **transferring** step, recording in said first device **information indicating that said transfer has occurred.**

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

at **a time substantially contemporaneous with** said **transferring** step,	- see above - "a time substantially contemporaneous with" is not used in the specification, and is indefinite.
recording in said first device **information indicating that said**	- "transfer" is indefinite, e.g., on how it differs, if at all, from "move" or "copy."

transfer has occurred.	- "information indicating that said transfer has occurred" is indefinite, e.g., on the extent to which the information identifies "said transfer," e.g., what was "transferred" and/or to what it was "transferred."

3) A method as in claim 2, in which:
a) said **information indicating that said transfer has occurred includes** an **encumbrance on said budget**.

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) said **information indicating that said transfer has occurred includes** an **encumbrance on said budget**.	- see above - "an encumbrance on said budget" is indefinite, e.g., for the same reasons that "budget" is indefinite, and, as to its function and structure, and on whether it must be uniquely identifiable with respect to the universe of "VDE" nodes.

4) A method as in claim 3, in which:
a) said **encumbrance operates to reduce the number of copies of said digital file authorized by said budget.**

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

said **encumbrance operates to reduce the number of copies of said digital file authorized by said budget.**	- see above - "operates to reduce the number of copies of said digital file authorized by said budget" is indefinite, e.g., on whether it reduces the total global number of "copies" that ever will have been made of that "file" at any time,

	by any "user," by any device, and for any length of persistence, and on meaning of an "encumbrance" "operating."

11) A method comprising:

2. **receiving** a digital **file**;

b) **storing** said digital **file in** a first **secure memory** of a first device;

c) **storing** information **associated with said digital file in a secure database** stored on said first device, said information **including** a first **control**;

d) **determining whether said digital file may be copied and stored on a second device based on said first control, said determining step** including **identifying said second device** and determining whether said first **control** allows **transfer** of **said copied file** to said second device, **said determination** based at least in part on **the features present at the device to which said copied file is to be transferred**;

e) **if said first control allows at least a portion of said digital file to be copied and stored on a second device,**

f) **copying at least a portion** of said digital **file**;

g) **transferring at least a portion** of said digital **file to a second device** including a **memory** and an **audio and/or video output**;

h) **storing said digital file in** said **memory** of said second device; and

2. **rendering said digital file** through said output.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file**;	- "receiving … file" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "file," and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file."
b) **storing** said digital **file in** a first **secure memory** of a first	- see above - "storing … in" is used inconsistently in the

device;	specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - if "secure memory" is not at least limited to the disclosed internal RAM and/or ROM (directly addressable by a SPU processor instruction) located within the physically protected, "tamper-resistant" SPU, the term "secure memory" would be indefinite. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure."
c) **storing** information **associated with said digital file in** a **secure database** stored on said first device,	- see above - if "associated with said digital file" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with said digital file" would be indefinite. - if "secure database" is not at least limited to the disclosed "secure database" (including its "secure database manager" and alleged access control "VDE" mechanisms), the term "secure database" would be indefinite.
said information **including** a first **control**	- see above - "including" is used inconsistently in the specification

	and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite.
d) **determining whether said digital file may be copied and stored on a second device based on said first control;**	- see above - "copied" is indefinite (see "copy" above) - "determining whether said digital file may be copied and stored on a second device" is indefinite, e.g., on whether this step determines whether the file may be "copied" on a second device. - "a second device" is indefinite, e.g., on whether it means "any" second device or a particular second device. - "determining whether said digital file may be copied and stored on a second device based on said first control" is indefinite; e.g., it is inconsistent with the later claim limitation "if said first control allows at least a portion of said digital file to be copied and stored on a second device"
said determining step including **identifying said second device** and determining whether said first **control** allows **transfer** of **said copied file** to said second device,	- see above - "identifying said second device" is indefinite, e.g., on whether the identification is of the type of device or of the particular second device unit, and on whether it is a unique identification. - "transfer" is indefinite, e.g., on how it differs, if at all, from "move" or "copy." - "said copied file" lacks antecedent basis, and is indefinite. For example, the preceding limitations do not recite the "copying" of any "file" that could be an

	antecedent for “ said copied file.” - if “copied file” is not at least limited to a “file” that has been “copied” at least once, then “copied file” would be indefinite.
said determination based at least in part on **the features present at the device to which said copied file is to be transferred;**	- “said determination” is indefinite as to its antecedent basis (e.g., “determining whether said digital file may be copied and stored …” or “determining whether said first control allows transfer ….”). - “the features present at the device” is indefinite, e.g., on whether “the features” means all or any particular type of features, on what has these “features,” and on the relationship, if any, of “features present at the device” to features of the device. - “to which said copied filed is to be transferred” is indefinite. For example, it is inconsistent with the other claim limitations reciting that “transfer” may not be allowed. - “transferred” is indefinite, e.g., on how it differs, if at all, from “moved.”
e) **if said first control allows at least a portion of said digital file to be copied** and stored on **a second device,**	- see above - “a portion of said digital file” is indefinite, e.g., on whether it encompasses or excludes matter that is merely referenced within the “file.” - “a second device” is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the “said second device” recited earlier in the claim. - depending on the construction of other claim limitations, such as “determining whether said digital file may be copied and stored on a second device based on said first control,” the phrase “if said first control allows at least a portion of said digital file to be copied and stored on a second device” may be inconsistent with

	other limitations of this claim, and thus may be indefinite.
f) **copying at least a portion** of said digital **file**;	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control."
g) **transferring at least a portion** of said digital **file to a second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "copied" in the preceding step. - "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the "said second device" recited earlier in the claim.
including a **memory**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
and an **audio and/or video output;**	- "audio and/or video output" is indefinite.
h) **storing said digital file in** said **memory** of said second device;	- see above - "storing said digital file" is indefinite and

and	inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."
i) **rendering said digital file** through **said output.**	- see above - "rendering said digital file" is indefinite and inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."

15) A method comprising:

2. **receiving** a digital **file**;

b) an **authentication step** comprising:

c) **accessing** at least one **identifier associated with a first device**; and

d) **determining whether said identifier is associated with a device and/or user authorized to store said digital file;**

e) **storing** said digital **file in** a first **secure memory** of said first device, **but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;**

f) **storing** information **associated with said digital file in** a **secure database** stored on said first device, said information **including** at least one **control**;

g) **determining whether said digital file may be copied and stored on a second device based on said at least one control;**

h) **if said at least one control allows at least a portion of said digital file to be copied** and stored on a **second device,**

2. **copying at least a portion** of said digital **file**;

j) **transferring at least a portion** of said digital **file** to a **second device** including a **memory** and an **audio and/or video output;**

k) **storing said digital file in** said **memory** of said second device; and

l) **rendering said digital file** through said output.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file;**	- "receiving … file" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "file," and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file."
b) an **authentication step** comprising:	- "authentication step" is indefinite, e.g., for the reasons set forth below.
c) **accessing** at least one **identifier associated with a first device or with a user of said first device**; and	- "accessing" is indefinite, e.g., on whether it encompasses or excludes ascertaining the information content of what is "accessed" (e.g., decrypting any encrypted information). - if "identifier" is not at least limited to a value that uniquely identifies a particular device or "user," it would be indefinite. - "identifier associated with" is indefinite, e.g., on whether the "identifier" is uniquely "associated with." - "identifier associated with a first device or with a user of said first device" is indefinite and inconsistent with the later claim recitation of "determining whether said identifier is associated with a device and/or user …." - "a user of said first device" is indefinite, e.g., on whether the "user" is a current, past, or potential "user" of the device.
d) **determining whether said identifier is associated with a device and/or user authorized to store said digital file;**	- "determining whether said identifier is associated with a device and/or user" is indefinite and inconsistent with the preceding claim limitation of an "identifier associated with a first device or with a user of said first device." - "authorized to store said digital file" is indefinite, e.g., on whether such "authorization" is conditional or

	unconditional.
e) **storing** said digital **file in** a first **secure memory** of said first device,	- see above - "storing … in" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - if "secure memory" is not at least limited to the disclosed internal RAM and/or ROM (directly addressable by a SPU processor instruction) located within the physically protected, "tamper-resistant" SPU, the term "secure memory" would be indefinite. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure."
but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;	- "said device and/or user" is indefinite and has an indefinite antecedent basis (e.g., "a device and/or user authorized to store said digital file" or "at least one identifier associated with a first device or with a user of said first device"). - "so authorized" is indefinite and has an indefinite antecedent basis (e.g., "authorized" for "storing said digital file in a first secure memory of said first device" or "authorized to store said digital file"). - "but only if said device and/or user is so authorized" is inconsistent with "but not proceeding with said storing if said device and/or user is not authorized," rendering both phrases indefinite.
f) **storing** information **associated with said digital file in** a **secure**	- see above - if "associated with said digital file" is not at least

database stored on said first device,	limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with said digital file" would be indefinite. - if "secure database" is not at least limited to the disclosed "secure database" (including its "secure database manager" and alleged access control "VDE" mechanisms), the term "secure database" would be indefinite.
said information **including** at least one **control**	- see above - "including" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite.
g) determining whether said digital file may be copied and stored on a second device based on said at least one control;	- see above - "copied" is indefinite (see "copy" above) - "determining whether said digital file may be copied and stored on a second device based on said at least one control" is indefinite, e.g., on whether this step determines whether the "file" may be "copied" on a second device. - "a second device" is indefinite, e.g., on whether it

	means "any" second device or a particular second device.
h) **if said at least one control allows at least a portion of said digital file to be copied** and stored on a **second device**,	- see above - "a portion of said digital file" is indefinite, e.g., on whether it encompasses or excludes matter that is merely referenced within the "file." - depending on the construction of other claim limitations, such as "determining whether said digital file may be copied and stored on a second device based on said at least one control," the phrase "if said at least one control allows at least a portion of said digital file to be copied" may be inconsistent with other limitations of this claim, and thus may be indefinite.
i) **copying at least a portion of** said digital **file**;	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "at least one control."
j) **transferring at least a portion** of said digital **file** to a **second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "at least one control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "copied" in the preceding step.

	- "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the same particular second device referred to earlier in the claim (to the extent the claim earlier refers to a particular second device).
including a **memory**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
and an **audio and/or video output**;	- "audio and/or video output" is indefinite.
h) **storing said digital file in** said **memory** of said second device; and	- see above - "storing said digital file" is indefinite and inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."
i) **rendering said digital file** through **said output**.	- see above - "rendering said digital file" is indefinite and inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."

19) A method comprising:

a) **receiving** a digital **file at** a first device;

b) **establishing communication between** said first device and a **clearinghouse** located at a **location remote from** said first device;

c) said first device obtaining **authorization information including** a key from said **clearinghouse**;

d) said first device using said **authorization information** to **gain access to or** make at least one **use** of said first digital **file**, including using said key to decrypt at least a portion of said first digital **file**; and

e) **receiving** a first **control** from said **clearinghouse at** said first device;

f) **storing** said first digital **file in** a **memory** of said first device;

g) using said first **control** to **determine whether said first digital file may be copied and stored on a second device;**

h) **if said first control allows at least a portion of said first digital file to be copied** and stored **on a second device,**

i) **copying at least a portion** of said first digital **file**;

j) **transferring at least a portion** of said first digital **file** to a **second device** including a **memory** and an **audio and/or video output**;

k) **storing** said first digital **file portion in** said **memory** of said second device; and

l) rendering said first digital **file portion** through **said output.**

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file at** a first device;	- "receiving … at" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file."
b) **establishing communication between** said first device and a **clearinghouse** located at a **location remote from** said first device;	- "establishing communication between" is indefinite, e.g., on whether this step requires one or more "communications," on whether two-way "communication" must be established, and on the nature of the "communication." - "location remote from" is indefinite, e.g., on how "remoteness" is determined. - "clearinghouse" is indefinite. For example, it vaguely suggests a function without suggesting any particular structure for performing such function. No particular corresponding structure is adequately described in the specification.
c) said first device obtaining	- if "authorization information" is not at least limited

authorization information including a key from said **clearinghouse**;	to (1) the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, and (2) the key and other data used thereby, the term "authorization information" would be indefinite. - "including" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference.
d) said first device using said **authorization information** to **gain access to or** make at least one **use** of said first digital **file**, including using said key to decrypt at least a portion of said first digital **file**; and	- "gain access to" is indefinite, e.g., on whether it encompasses or excludes ascertaining the information content of what is "accessed" (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying."
e) **receiving** a first **control** from said **clearinghouse at** said first device;	- see above - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite.
f) **storing** said first digital **file in** a **memory** of said first device;	- see above - "storing … in" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
g) using said first **control** to **determine whether said first**	- see above - "copied" is indefinite, e.g., on whether it

digital file may be copied and stored on a second device;	encompasses or excludes creating something that is not an identical duplicate of the original; and if it does encompass that, then how clear that something must be to the original to constitute a "copy." - "determine whether said first digital file may be copied and stored on a second device" is indefinite, e.g., on whether this step determines whether the "file" may be "copied" on a second device. - "a second device" is indefinite, e.g., on whether it means "any" second device or a particular second device. - "using said first control to determine whether said first digital file may be copied and stored on a second device" is indefinite; e.g., it is inconsistent with the later claim limitation "if said first control allows at least a portion of said first digital file to be copied and stored on a second device"
h) **if said first control allows at least a portion of said first digital file to be copied and stored on a second device,**	- see above - "a portion of said digital file" is indefinite, e.g., on whether it encompasses or excludes matter that is merely referenced within the "file." - depending on the construction of other claim limitations, such as "using said first control to determine whether said first digital file may be copied and stored on a second device" the phrase "if said first control allows at least a portion of said first digital file to be copied" may be inconsistent with other limitations of this claim, and thus may be indefinite.
i) **copying at least a portion of** said first digital **file;**	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be

	to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control."
j) **transferring at least a portion** of said first digital **file** to a **second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a portion not "copied" in the preceding step. - "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the same particular second device referred to earlier in the claim (to the extent the claim earlier refers to a particular second device).
including a **memory**	- see above
and an **audio and/or video output**;	- "audio and/or video output" is indefinite.
k) **storing** said first digital **file portion in** said **memory** of said second device; and	- see above
l) rendering said first digital **file portion** through **said output**.	- see above

<u>'683</u>

2. A system including:

a **first apparatus including,**
user controls,
a communications port,
a processor,
a **memory storing:**
a first **secure container containing a governed item**, the first **secure container governed item** being at least in part encrypted; the first **secure container having been received from a second apparatus;**
a first **secure container rule at least in part governing an aspect of access to or use of** said first **secure container governed item, the first secure container rule**, the first **secure container rule having been received from a third apparatus** different from said second apparatus; and
hardware or software used for receiving and opening secure containers,said **secure containers** each **including the capacity to contain a governed item, a secure container rule being associated with** each of said **secure containers**;
a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus,** said **protected processing environment** including **hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container**; and
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

2. A system including:	
a **first apparatus including,**	- the claim is indefinite on which of the recited elements are included in the "first apparatus."
user controls,	- "user controls" is indefinite.
a communications port,	
a processor,	
a **memory storing:**	- "memory" is indefinite, e.g., on whether it

	encompasses or excludes storage that is not directly addressable by the processor. - "storing" is used inconsistently in at least the allegedly incorporated specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - the claim is indefinite on which of the recited elements are "stored" in the "memory."
a first **secure container** **containing a governed item,**	- "secure container" is indefinite, e.g., on its structure and certain of its functions, on whether it encompasses or excludes "virtual container." The specification does not disclose adequate corresponding structure under Section 112, ¶ 6. - "container" is indefinite, e.g., on its structure and certain of its functions, and on what distinguishes a single "container" from two separate "containers." - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure." - "storing … secure container" is indefinite, e.g., on what part, if any, of the "container" may merely be referenced from within the memory. - "containing" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "containing."

	- if "govern" is not at least limited to preventing unapproved user processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific users, the term "governed" (and "governed item") would be indefinite. - "a governed item," is indefinite, e.g., on what distinguishes "a governed item" from two separate governed items.
the first **secure container** **governed item** being at least in part encrypted;	- see above
the first **secure container** **having been received from a second apparatus;**	- see above - "received" is indefinite, e.g., on what processing, if any, is required to complete this "receipt," and on what "received" the "received" item. - "having been received from" recites the (possibly unknowable) history of a component (or something stored in a component) rather than the structure or function of the component, apparatus or system, thereby rendering this apparatus claim indefinite. - "received from a second apparatus" is indefinite, e.g., on whether this encompasses or excludes receipt from some intermediary between the second apparatus and first apparatus.
a first **secure container rule at least in part governing an**	- see above - "rule" is indefinite and is used inconsistently in the

aspect of access to or use of said first secure container governed item,	specification. For example, the relationship between a "rule" and a "control" is indefinite. - "secure container rule" is indefinite and not used in the specification. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "governing." - if "governing" is not at least limited to preventing unapproved user processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific users, the term "governing" would be indefinite. - "at least in part governing" is indefinite, e.g., on how to identify when this act of "governing" has begun, is ongoing, or has ended. - "access" is indefinite, e.g., on whether it encompasses or excludes determining the information content of what is "accessed" (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the allegedly incorporated specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying." - "an aspect of access to or use of" is indefinite.
the first secure container rule,	- see above - the claim is indefinite on the significance of this repetition of the phrase "the first secure container rule."

the first **secure container rule having been received from a third apparatus** different from said second apparatus; and	- see above - "received from a third apparatus" is indefinite, e.g., on whether this encompasses or excludes receipt from some intermediary between the third apparatus and first apparatus.
hardware or software used for receiving and opening secure containers,	- see above - "receiving" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "secure containers," and on what or where they are received from. - if "opening secure containers" is not at least limited to successful completion of the "OPEN method" expressly disclosed in the allegedly incorporated specification, the phrase "opening secure containers" would be indefinite. - "hardware or software used for receiving and opening secure containers," is indefinite, e.g., on the structure of this "hardware or software," and on whether the same "hardware or software" performs both "receiving" and "opening." The specification does not disclose adequate corresponding structure.
said **secure containers** each **including the capacity to contain a governed item,**	- see above - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" would be indefinite. - "contain" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does

	encompass merely holding a reference, what type of reference suffices to constitute "contain." - "including the capacity to contain a governed item" is indefinite, e.g., on the manner in which a "capacity" is included in a "secure container," and on whether the "capacity to contain" must apply to some particular "governed item" or to every "governed item" without limitation.
a secure container rule being associated with each of said secure containers;	- see above - if "being associated with … secure containers" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific users, the phrase "being associated with … secure containers" would be indefinite. - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" is indefinite.
a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus,	- "protected" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?), and on the nature and the level(s) of protection from those threats that separate(s) "protected" from "not protected."

	- if "protected processing environment" is not at least limited to excluding the processor and "memory" recited earlier in the claim, and is not at least limited to executing software and/or hardware (if any) expressly disclosed in the specification and identified as a "protected processing environment," the term "protected processing environment" would be indefinite. - if "protecting" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "protecting" would be indefinite. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "protecting." - "information contained in said protected processing environment" is indefinite, e.g., on what aspects of a "protected processing environment" can "contain" information, and on whether "contain" encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "protecting from … tampering" is indefinite, e.g., on the specific threat(s) being addressed, and on the level(s) and nature of protection from those threats. - "a user of said first apparatus" is indefinite, e.g., on whether "a user" means "any user" or a particular "user."

said **protected processing environment** including **hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container**; and	- see above - "said first secure container rule and a second secure container rule" is indefinite, e.g., on what distinguishes a single "rule" from two separate "rules." - "hardware or software used for applying ... in a secure container" is indefinite, e.g., on the structure of this "hardware or software." The specification does not disclose adequate corresponding structure. - "applying ... in combination" is indefinite, e.g., on the manner in which the "rules" are merged and applied. - "contained in" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference in, and, if it does encompass merely holding a reference in, what type of reference suffices to constitute "contained in." - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "govern." - if "govern" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "govern" would be indefinite. - "a governed item contained in a secure container" is indefinite and has no or an indefinite antecedent basis as both "a governed item" and "a secure container."

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	- see above - "hardware or software used for transmission ... or for the receipt ... from other apparatuses" is indefinite, e.g., on the structure of this "hardware or software," and on its relationship, if any, with the previously recited "hardware or software used for receiving and opening secure containers," and on its relationship, if any, with any other element recited in the claim. The specification does not disclose adequate corresponding structure.

28. A system including;

a first apparatus including;

user controls,

a communications port,

a processor,

a **memory containing a** first **rule,**

hardware or software used for receiving and opening secure containers,said secure containers each **including the capacity to contain a governed item, a secure container rule being associated with** each of said secure containers;

a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said **protected processing environment** including **hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and

a second apparatus including:

user controls,

a communications port,

a processor,

a **memory containing a** second **rule,**

hardware or software used for receiving and opening secure containers,said **secure containers** each **including the capacity to contain a governed item**, a **secure container rule being associated with** each of said **secure containers**;

a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus**, said **protected processing environment** including **hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**;

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and

an **electronic intermediary**, said **intermediary** including a **user rights authority clearinghouse**.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

28. A system including:	
a first apparatus including,	- the claim is indefinite on which of the recited elements are included in the "first apparatus."
user controls,	- "user controls" is indefinite.
a communications port,	
a processor,	
a **memory containing** a first **rule,**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor. - "containing" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "containing." - "rule" is indefinite and is used inconsistently in the specification. For example, the relationship between a

	"rule" and a "control" is indefinite.
hardware or software used for receiving and opening secure containers,	- see above - "receiving" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "secure containers," and on what or where they are received from. - if "opening secure containers" is not at least limited to successful completion of the "OPEN method" expressly disclosed in the allegedly incorporated specification, the phrase "opening secure containers" would be indefinite. - "secure container" is indefinite, e.g., on its structure and certain of its functions, and on whether it encompasses or excludes "virtual container." The specification does not disclose adequate corresponding structure under Section 112, ¶ 6. - "container" is indefinite, e.g., on its structure and certain of its functions, and on what distinguishes a single "container" from two separate "containers." - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure." - "hardware or software used for receiving and opening secure containers," is indefinite, e.g., on the structure of this "hardware or software," and on whether the same "hardware or software" performs both "receiving" and "opening." The specification does not disclose adequate corresponding structure.

said secure containers each **including the capacity to contain a governed item,**	- see above - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" would be indefinite. - "contain" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "a governed item," is indefinite, e.g., on what distinguishes "a governed item" from two separate "governed items." - "including the capacity to contain a governed item" is indefinite.
a secure container rule being associated with each of **said secure containers**;	- see above - if "associated with ... secure containers" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with … secure containers" would be indefinite. - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able

	to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" is indefinite.
a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus,	- "protected" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "protected" from "not protected." - if "protected processing environment" is not at least limited to excluding the processor and "memory" recited earlier in the claim, and is not at least limited to executing software and/or hardware (if any) expressly disclosed in the specification and identified as a "protected processing environment," the term "protected processing environment" would be indefinite. - if "protecting" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "protecting" would be indefinite. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "protecting." - "information contained in said protected processing environment" is indefinite, e.g., on what aspects of a

	"protected processing environment" can "contain" information, and on whether "contain" encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "protecting from … tampering" is indefinite, e.g., on the specific threat(s) being addressed and on the level(s) and nature of protection from those threats. - "a user of said first apparatus" is indefinite, e.g., on whether "a user" means "any user" or a particular "user."
said **protected processing environment** including **hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and	- see above - "said first rule and a secure container rule" is indefinite, e.g., on whether "a secure container rule" is separate from a "first rule," and on what distinguishes a single "rule" from two separate "rules." - "hardware or software used for applying … in a secure container," is indefinite, e.g., on the structure of this "hardware or software." The specification does not disclose adequate corresponding structure. - "applying … in combination" is indefinite, e.g., on the manner in which the "rules" are merged and applied. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "govern." - if "govern" is not at least limited to preventing unapproved user processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular

	level), and specific "users," the term "govern" would be indefinite. - "access" is indefinite, e.g., on whether it encompasses or excludes determining the information content of what is accessed (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the allegedly incorporated specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying." - "an aspect of access to or use of" is indefinite. - "a governed item" is indefinite and has no or an indefinite antecedent.
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	- see above - "hardware or software used for transmission … or for the receipt … from other apparatuses" is indefinite, e.g., on the structure of this "hardware or software," on its relationship, if any, with the previously recited "hardware or software used for receiving and opening secure containers," on whether the same "hardware or software" performs both, and on its relationship, if any, with any other element recited in the claim. The specification does not disclose adequate corresponding structure.
a **second apparatus including,**	- the claim is indefinite on which of the recited elements are included in the "second apparatus." - the claim is indefinite for failing to link the first apparatus with the second apparatus in any manner.
user controls,	- "user controls" is indefinite.
a communications port,	
a processor,	
a **memory containing** a second	- "memory" is indefinite, e.g., on whether it

rule,	encompasses or excludes storage that is not directly addressable by the processor. - "containing" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "containing." - "rule" is indefinite and is used inconsistently in the specification. For example, it is indefinite on what distinguishes a single "rule" from two separate "rules."
hardware or software used for receiving and opening secure containers,	- see above - "receiving" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "secure containers," and on what or where they are received from. - if "opening secure containers" is not at least limited to successful completion of the "OPEN method" expressly disclosed in the allegedly incorporated specification, the phrase "opening secure containers" would be indefinite. - "secure container" is indefinite, e.g., on its structure and certain of its functions, and on whether it encompasses or excludes "virtual container." The specification does not disclose adequate corresponding structure under Section 112, ¶ 6. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from

	those threats that separate(s) "secure" from "not secure." - "hardware or software used for receiving and opening secure containers," is indefinite, e.g., on the structure of this "hardware or software," and on whether the same hardware or software performs both "receiving" and "opening." The specification does not disclose adequate corresponding structure.
said secure containers each including the capacity to contain a governed item,	- see above - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" would be indefinite. - "contain" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "a governed item," is indefinite, e.g., on what distinguishes "a governed item" from two separate governed items. - "including the capacity to contain a governed item" is indefinite.
a secure container rule being associated with each of said secure containers;	- see above - if "associated with ... secure containers" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between

	specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with ... secure containers" would be indefinite. - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" is indefinite.
a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus,	- "protected" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "protected" from "not protected." - if "protected processing environment" is not at least limited to excluding the processor and "memory" recited earlier in the claim, and is not at least limited to executing software and/or hardware (if any) expressly disclosed in the specification and identified as a "protected processing environment," the term "protected processing environment" would be indefinite. - if "protecting" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific

	"objects" (and their content at an arbitrary granular level), and specific "users," the term "protecting" would be indefinite. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "protecting." - "information contained in said protected processing environment" is indefinite, e.g., on what aspects of a "protected processing environment" can "contain" information, and on whether "contain" encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "protecting from … tampering" is indefinite, e.g., on the specific threat(s) being addressed and on the level(s) and nature of protection from those threats. - "a user of said apparatus" is indefinite, e.g., on whether "a user" means "any user" or a particular "user," and on whether "said apparatus" is the first or second apparatus.
said **protected processing environment** including **hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and	- see above - "said second rule and a secure container rule" is indefinite, e.g., on what distinguishes a single "rule" from two separate "rules." - "hardware or software used for applying … in a secure container," is indefinite, e.g., on the structure of this "hardware or software." The specification does not disclose adequate corresponding structure. - "applying … in combination" is indefinite, e.g., on the manner in which the rules are merged and applied. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "govern." - if "govern" is not at least limited to preventing

	unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "govern" would be indefinite. - "access" is indefinite, e.g., on whether it encompasses or excludes determining the information content of what is "accessed" (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the allegedly incorporated specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying." - "an aspect of access to or use of" is indefinite. - "a governed item" is indefinite and has no or an indefinite antecedent.
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	- see above - "hardware or software used for transmission ... or for the receipt ... from other apparatuses" is indefinite, e.g., on the structure of this "hardware or software," and on its relationship, if any, with the previously recited "hardware or software used for receiving and opening secure containers," and on its relationship, if any, with any other element recited in the claim. The specification does not disclose adequate corresponding structure.
an **electronic intermediary**, said **intermediary** including a **user**	- see above - "electronic intermediary" is indefinite, e.g., as to the

rights authority clearinghouse.	nature of its structure and function, and its relationship, if any, to either the first apparatus or the second apparatus, or to any other element of the claim, and on whether it encompasses or excludes a "virtual intermediary" or "virtual go-between." The specification does not disclose adequate corresponding structure. - "rights" is indefinite. - "user rights authority clearinghouse" is indefinite, e.g., as to the nature of its structure and function, and its relationship, if any, to either the first apparatus or the second apparatus, or to any other element of the claim. The specification does not disclose adequate corresponding structure.

29. A system as in claim 28, said **user rights authority clearinghouse** **operatively connected to make rights available to users.**

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

A system as in claim 28, said **user rights authority clearinghouse** **operatively connected to make rights available to users.**	- see above - "operatively connected" is indefinite, e.g., as to what it is connected. - "to make rights available to users" is indefinite, e.g., on which "users" it addresses and what it means for "rights" to be "available" to those "users."

Enablement and Written Description Invalidity of the Asserted InterTrust Patent Claims

Each of the asserted InterTrust patent claims is invalid for violating the written description and enablement requirements of 35 U.S.C. § 112, ¶ 1, particularly as the claims are construed in the untenable manner apparently underlying InterTrust's infringement accusations in this action.

One way in which the claims of the '193 patent and the '683 patent (including but not limited to the extent the allegedly incorporated applications are considered) are not enabled is that the applications from which they issued are so rambling, unfocused, vague and internally inconsistent that they obfuscated any alleged teaching of the claimed subject matter and failed to enable one of skill in the art, without undue experimentation, to follow any alleged directions of the application to carry out the claimed subject matter.

The claims are invalid for violating the written description requirement to the extent that they are construed so as to contradict and/or not require the essential, non-optional alleged attributes of the alleged "invention" that were identified in the application (as originally filed, disregarding all new matter) from which the claims issued. Those disclosed "invention" defining statements include descriptions of the "present invention" and/or "VDE" or "virtual distribution environment," statements distinguishing prior techniques or products, such statements in the Summary of the Invention or Objects of the Invention sections of the application, and non-optional attributes shared by the disclosed embodiments and/or initial application claims. They include, but are not limited to, such alleged attributes reflected in the below-listed exemplary statements in the applications filed on December 9, 1998 (the '193 Patent), December 28, 1998 (the '683 Patent), and/or similar statements in the patents' Patent Office prosecution histories and/or any properly incorporated patent(s) or patent application(s), if any.

The claims are further invalid under the enablement requirement as the applications did not enable those of skill in the art to build systems having these touted attributes, at least not without an unreasonable amount of experimentation.

- "The present invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway."
- "The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted

by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems."

- "VDE may be used to provide basic usage control in several ways. First, it permits the "embedding" of multiple containers within a single object. Embedded objects permit the "nesting" of control structures within a container. VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) and provides flexible control information over any action associated with the information which can be described as a VDE controlled process."

- "Providers of "electronic currency" have also created protections for their type of content. These systems are not sufficiently adaptable, efficient, nor flexible enough to support the generalized use of electronic currency. Furthermore, they do not provide sophisticated auditing and control configuration capabilities. This means that current electronic currency tools lack the sophistication needed for many real- world financial business models. VDE provides means for anonymous currency and for "conditionally" anonymous currency, wherein currency related activities remain anonymous except under special circumstances."

- "Traditional content control mechanisms often require users to purchase more electronic information than the user needs or desires. For example, infrequent users of shrink-wrapped software are required to purchase a program at the same price as frequent users, even though they may receive much less value from their less frequent use. Traditional systems do not scale cost according to the extent or character of usage and traditional systems can not attract potential customers who find that a fixed price is too high. Systems using traditional mechanisms are also not normally particularly secure. For example, shrink-wrapping does not prevent the constant illegal pirating of software once removed from either its physical or electronic package."

- "Traditional electronic information rights protection systems are often inflexible and inefficient and may cause a content provider to choose costly distribution channels that increase a product's price. In general these mechanisms restrict product pricing, configuration, and marketing flexibility. These compromises are the result of techniques for controlling information which cannot accommodate both different content models and content models which reflect the many, varied requirements, such as content delivery strategies, of the model participants. This can limit a provider's ability to deliver sufficient overall value to justify a given product's cost in the eyes of many potential users. VDE allows content providers and distributors to create applications and distribution networks that reflect content providers' and users' preferred business models. It offers users a uniquely cost effective and feature rich system that supports the ways providers want to distribute information and the ways users want to use such information."

- "VDE provides important enhancements for improving data security in organizations by providing "smart" transaction management features that can be far more effective than key and password based "go/no go" technology."

- "A variety of capabilities are required to implement an electronic commerce environment. VDE is the first system that provides many of these capabilities and therefore solves fundamental problems related to electronic dissemination of information."

- "The scalable transaction management/auditing technology of the present invention will result in more efficient and reliable interoperability amongst devices functioning in electronic commerce and/or data security environments."

- "Templates, classes (including user groups employing an object under group access), and flexible control structures including object "independent" permissions records (permissions that can be associated with a plurality of objects) and structures that support budgeting and auditing as separate VDE processes, help focus the flexible and configurable capabilities inherent within authoring provided by the present invention in the context of specific industries and/or businesses and/or applications. ... The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, ... the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment."

- "The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances."

- "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable."

- "A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information (normally in the form of VDE objects containing one or more methods, data, or load module VDE components). This independently delivered control information can be integrated with senior and other pre-existing content control information to securely form derived control information using the negotiation mechanisms of the present invention. All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. This means that, for example, all load modules and any mediating data which are listed by the derived control information as required must be available and securely perform their required function."

- "A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model). This shaping can occur as content control information passes from one VDE participant to another and to the extent allowed by "in place" content control information. This process allows users of VDE to recast existing control information and/or add new control information as necessary (including the elimination of no longer required elements)."

- "VDE's fundamental configurability will allow a broad range of competitive electronic commerce business models to flourish."

- "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/or otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well."

- "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers. Such capabilities allow VDE supported product models to evolve by progressively reflecting the requirements of "next" participants in an electronic commercial model."

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (a) integration into the fundamental control environment of a broad range of electronic appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any electronic appliance environment while maintaining overall system security;"

- "Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment."

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (c) generic content model;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (b) modular data structures;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (d) general modularity and independence of foundation architectural components;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (e) modular security structures;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (f) variable length and multiple branching chains of control; and"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (g) independent, modular control structures in the form of executable load modules that can be maintained in one or more libraries, and assembled into control methods and models, and where such model control schemes can "evolve" as control information passes through the VDE installations of participants of a pathway of VDE content control information handling."

- "An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, VDE includes features that: … "sufficiently" impede unauthorized and/or uncompensated use of electronic information and/or appliances through the use of secure communication, storage, and transaction management technologies …."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, … support low-cost, efficient, and effective security architectures for transaction control, auditing, reporting, and related communications and information storage …."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, … support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, … securely store at a user's site potentially highly detailed information reflective of a user's usage of a variety of different content segment types… support trusted chain of handling capabilities for pathways of distributed electronic information and/or for content usage related information."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support flexible auditing mechanisms, such as employing "bitmap meters, ..."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support "launchable" content, that is content that can be provided by a content provider to an end-user, who can then copy or pass along the content to other end-user parties without requiring the direct participation of a content provider to register and/or otherwise initialize the content for use ...."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... securely support electronic currency and credit usage control, storage, and communication at, and between, VDE installations."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide smart object agents that can carry requests, data, and/or methods, including budgets, authorizations, credit or currency, and content. ... Smart objects can, for example, be transmitted to a remote location to perform a specified database search on behalf of a user ...."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... "employ "templates" to ease the process of configuring capabilities of the present invention as they relate to specific industries or businesses. ...Given the very large range of capabilities and configurations supported by the present invention, reducing the range of configuration opportunities to a manageable subset particularly appropriate for a given business model allows the full configurable power of the present invention to be easily employed by "typical" users who would be otherwise burdened with complex programming and/or configuration design responsibilities template applications can also help ensure that VDE related processes are secure and optimally bug free by reducing the risks associated with the contribution of independently developed load modules, including unpredictable aspects of code interaction between independent modules and applications, as well as security risks associated with possible presence of viruses in such modules. ... As the context surrounding these templates changes or evolves, template applications provided under the present invention may be modified to meet these changes for broad use, or for more focused activities. ... Of course, templates may, under certain circumstances have fixed control information and not provide for user selections or parameter data entry."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms to persistently maintain trusted content usage and reporting control information through both a sufficiently secure chain of handling of content and content control information and through various forms of usage of such content wherein said persistence of control may survive such use. Persistence of control includes the ability to extract information from a VDE container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or VDE installation control information stipulates should persist and/or control usage of content in the newly formed container. Such control information can continue to manage usage of container content if the container is "embedded" into another VDE managed object, such as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, … enables users … to specify preferences or requirements related to their use of electronic content and/or appliances. Content users, such as end-user customers using commercially distributed content … can define, if allowed by senior control information, budgets, and/or other control information, to manage their own internal use of content. Uses include, for example, a user setting a limit on the price for electronic documents that the user is willing to pay without prior express user authorization, and the user establishing the character of metering information he or she is willing to allow to be collected (privacy protection)."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, … provide mechanisms that allow control information to "evolve" and be modified according, at least in part, to independently, securely delivered further control information. … Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content)."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, … support multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... enable a user to securely extract, through the use of the secure subsystem at the user's VDE installation, at least a portion of the content included within a VDE content container to produce a new, secure object (content container), such that the extracted information is maintained in a continually secure manner through the extraction process."

- "it is important to provide a framework of operation and/or structure to allow existing industries and/or applications and/or businesses to manipulate familiar concepts related to content types, distribution approaches, pricing mechanisms, user interactions with content and/or related administrative activities, budgets, and the like."

- "The present invention allows content providers and users to formulate their transaction environment to accommodate:

- (1) desired content models, content control models, and content usage information pathways,
- (2) a complete range of electronic media and distribution means,
- (3) a broad range of pricing, payment, and auditing strategies,
- (4) very flexible privacy and/or reporting models,
- (5) practical and effective security architectures, and
- (6) other administrative procedures that together with steps (1) through (5) can enable most "real world" electronic commerce and data security models, including models unique to the electronic world."

- "This ability of the present invention to support multiple pathway branches for the flow of both VDE content control information and VDE managed content enables an electronic commerce marketplace which supports diverging, competitive business partnerships, agreements, and evolving overall business models which can employ the same content properties combined, for example, in differing collections of content representing differing at least in part competitive products."

- "the present invention can help ensure, for example, that parties, will be paid for use of distributed information in a manner consistent with their agreement; … the present invention can, for example, help ensure that data is used only in authorized ways; …."

- "The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, to allow for efficient adaptation into new industries as they evolve, and to reflect the evolution and/or change of an existing industry and/or business, as well as to support one or more groups of users who may be associated with certain permissions and/or budgets and object types. The flexibility of VDE templates, classes, and basic control structures is enhanced through the use of VDE aggregate and control methods which have a compound, conditional process impact on object control. Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment. Thus, the present invention fully supports the requirements and biases of content providers without forcing them to fit a predefined application model. It allows them to define the rights, control information, and flow of their content (and the return of audit information) through distribution channels."

- "a creator … may allow changes by an auditor for event trails, but not allow anyone but themselves to read those trails …."

- "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced. As a result, the creator and/or distributor and/or client administrator and/or other contributor of secure control information for each property (for example, an end-user restricting the kind of audit information he or she will allow to be reported and/or a financial clearinghouse establishing certain criteria for use of its credit for payment for use of distributed content) can be confident that their contributed and accepted control information will be enforced (within the security limitations of a given VDE security implementation design)."

- "Since different groups of components can be put together for different applications, the present invention can provide electronic control information for a wide variety of different products and markets. This means the present invention can provide a "unified," efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as a single standard for electronic rights protection, data security, and electronic currency and banking."

- "In a VDE, the separation between a rights application and its foundation permits the efficient selection of sets of control information that are appropriate for each of many different types of applications and uses."

- "Due to its open design, VDE allows (normally under securely controlled circumstances) applications using technology independently created by users to be "added" to the system and used in conjunction with the foundation of the invention."

- "In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity."

- "VDE permits multiple, separate electronic arrangements to be formed between subsets of parties in a VDE supported electronic value chain model. These multiple agreements together comprise a VDE value chain "extended" agreement. VDE allows such constituent electronic agreements, and therefore overall VDE extended agreements, to evolve and reshape over time as additional VDE participants become involved in VDE content and/or appliance control information handling. VDE electronic agreements may also be extended as new control information is submitted by existing participants. With VDE, electronic commerce participants are free to structure and restructure their electronic commerce business activities and relationships. As a result, the present invention allows a competitive electronic commerce marketplace to develop since the use of VDE enables different, widely varying business models using the same or shared content."

- "A feature of the present invention enables such flexibility of metering control mechanisms to accommodate a simultaneous, broad array of: (a) different parameters related to electronic information content use; (b) different increment units (bytes, documents, properties, paragraphs, images, etc.) and/or other organizations of such electronic content; and/or (c) different categories of user and/or VDE installation types, such as client organizations, departments, projects, networks, and/or individual users, etc. This feature of the present invention can be employed for ...."

- "A feature of the present invention provides for payment means supporting flexible electronic currency and credit mechanisms, including the ability to securely maintain audit trails reflecting information related to use of such currency or credit."

- "Features of the present invention help ensure that a requirement that a clearinghouse report such usage information and payment content will be observed."

- "A feature of the present invention is the use of portable VDEs as transaction cards at retail and other establishments, wherein such cards can "dock" with an establishment terminal that has a VDE secure sub-system and/or an online connection to a VDE secure and/or otherwise secure and compatible subsystem, such as a "trusted" financial clearinghouse (e.g., VISA, Mastercard)."

- "A feature of VDE provided by the present invention is that certain one or more methods can be specified as required in order for a VDE installation and/or user to be able to use certain and/or all content. For example, a distributor of a certain type of content might be allowed by "senior" participants (by content creators, for example) to require a method which prohibits end-users from electronically saving decrypted content, a provider of credit for VDE transactions might require an audit method that records the time of an electronic purchase, and/or a user might require a method that summarizes usage information for reporting to a clearinghouse (e.g. billing information) in a way that does not convey confidential, personal information regarding detailed usage behavior. A further feature of VDE provided by the present invention is that creators, distributors, and users of content can select from among a set of predefined methods (if available) to control container content usage and distribution functions and/or they may have the right to provide new customized methods to control at least certain usage functions (such "new" methods may be required to be certified for trustedness and interoperability to the VDE installation and/or for of a group of VDE applications). As a result, VDE provides a very high degree of configurability with respect to how the distribution and other usage of each property or object (or one or more portions of objects or properties as desired and/or applicable) will be controlled."

- "the present invention's trusted/secure, universe wide, distributed transaction control and administration system."

- "The configurability provided by the present invention is particularly critical for supporting electronic commerce, that is enabling businesses to create relationships and evolve strategies that offer competitive value. Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce products (and services) that meet both basic requirements and evolving needs of most commerce applications."

- "Templates, classes (including user groups employing an object under group access), and flexible control structures including object "independent" permissions records (permissions that can be associated with a plurality of objects) and structures that support budgeting and auditing as separate VDE processes, help focus the flexible and configurable capabilities inherent within authoring provided by the present invention in the context of specific industries and/or businesses and/or applications. ... The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, ... the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment."

- "As with the content control information for most VDE managed content, features of the present invention allows [sic] the content's control information to: (a) "evolve," for example, the extractor of content may add new control methods and/or modify control parameter data, such as VDE application compliant methods, to the extent allowed by the content's in-place control information. ... (b) allow a user to combine additional content with at least a portion of said extracted content, ... (c) allow a user to securely edit at least a portion of said content while maintaining said content in a secure form within said VDE content container; ... (d) append extracted content to a pre-existing VDE content container object and attach associated control information ... (e) preserve VDE control over one or more portions of extracted content after various forms of usage of said portions ... Generally, the extraction features of the present invention allow users to aggregate and/or disseminate and/or otherwise use protected electronic content information extracted from content container sources while maintaining secure VDE capabilities thus preserving the rights of providers in said content information after various content usage processes."

- "For example, features of the present invention include: (a) VDE system software to in part extend and/or modify host operating systems such that they possesses VDE capabilities, such as enabling secure transaction processing and electronic information storage; (b) one or more application programs that in part represent tools associated with VDE operation; and/or (c) code to be integrated into application programs, wherein such code incorporates references into VDE system software to integrate VDE capabilities and makes such applications VDE aware …."

- "The distribution control information provided by the present invention allow flexible positive control. No provider is required to include any particular control, or use any particular strategy, except as required by senior control information. Rather, the present invention allows a provider to select from generic control components (which may be provided as a subset of components appropriate to a provider's specific market, for example, as included in and/or directly compatible with, a VDE application) to establish a structure appropriate for a given chain of handling/control."

- "In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification."

- "Control methods are created primarily through the use of one or more of said executable, reusable load module code pieces (normally in the form of executable object components) and associated data. The component nature of control methods allows the present invention to efficiently operate as a highly configurable content control system. Under the present invention, content control models can be iteratively and asynchronously shaped, and otherwise updated to accommodate the needs of VDE participants to the extent that such shaping and otherwise updating conforms to constraints applied by a VDE application, if any (e.g., whether new component assemblies are accepted and, if so, what certification requirements exist for such component assemblies or whether any or certain participants may shape any or certain control information by selection amongst optional control information (permissions record) control methods. This iterative (or concurrent) multiple participant process occurs as a result of the submission and use of secure, control information components (executable code such as load modules and/or methods, and/or associated data)."

- "The special purpose secure circuitry provided by the present invention includes at least one of: a dedicated semiconductor arrangement known as a Secure Processing Unit (SPU) and/or a standard microprocessor, microcontroller, and/or other processing logic that accommodates the requirements of the present invention and functions as an SPU."
- "VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing,.reporting, and payment operating environment. VDE is not limited to being an application or application specific toolset that covers only a limited subset of electronic interaction activities and participants. Rather, VDE supports systems by which such applications can be created, modified, and/or reused. As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components. VDE can support a single electronic "world" within which most forms of electronic transaction activities can be managed."
- "A fundamental problem for electronic content providers is extending their ability to control the use of proprietary information. Content providers often need to limit use to authorized activities and amounts. Participants in a business model involving, for example, provision of movies and advertising on optical discs may include actors, directors, script and other writers, musicians, studios, publishers, distributors, retailers, advertisers, credit card services, and content end-users. These participants need the ability to embody their range of agreements and requirements, including use limitations, into an "extended" agreement comprising an overall electronic business model. This extended agreement is represented by electronic content control information that can automatically enforce agreed upon rights and obligations. Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE,

electronic commerce can function in the same way as traditional commerce-that is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties."

- "VDE allows the owners and distributors of electronic digital information to reliably bill for, and securely control, audit, and budget the use of, electronic information. It can reliably detect and monitor the use of commercial information products."

- "VDE provides comprehensive and configurable transaction management, metering and monitoring technology."

- "Protecting the rights of electronic community members involves a broad range of technologies. VDE combines these technologies in a way that creates a "distributed" electronic rights protection "environment." This environment secures and protects transactions and other processes important for rights protection. VDE, for example, provides the ability to prevent, or impede, interference with and/or observation of, important rights related transactions and processes."

- "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users."

- "VDE provides a unified solution that allows all content creators, providers, and users to employ the same electronic rights protection solution. ... VDE can allow content to be exchanged "universally" and users of an implementation of the present invention can interact electronically without fear of incompatibilities in content control, violation of rights, or the need to get, install, or learn a new content control system."

- "In addition, VDE:

- (a) is very configurable, modifiable, and re-usable;

- (b) supports a wide range of useful capabilities that may be combined in different ways to accommodate most potential applications;

- (c) operates on a wide variety of electronic appliances ranging from hand-held inexpensive devices to large mainframe computers;

- (d) is able to ensure the various rights of a number of different parties, and a number of different rights protection schemes, simultaneously;

- (e) is able to preserve the rights of parties through a series of transactions that may occur at different times and different locations;

- (f) is able to flexibly accommodate different ways of securely delivering information and reporting usage; and

- (g) provides for electronic analogues to "real" money and credit, including anonymous electronic cash, to pay for products and services and to support personal (including home) banking and other financial activities."

- "Users of VDE will not require additional rights protection systems for different information highway products and rights problems--nor will they be required to install and learn a new system for each new information highway application... The content and control information supplied by one group can be used by people who normally use content and control information supplied by a different group. VDE can allow content to be exchanged "universally" and users of an implementation of the present invention can interact electronically without fear of incompatibilities in content control, violation of rights, or the need to get, install, or learn a new content control system."

- "[VDE] can protect electronic rights including: (d) the privacy rights of users of content, ..."

- "Secure VDE hardware (also known as SPUs for Secure Processing Units), or VDE installations that use software to substitute for, or complement, said hardware (provided by Host Processing Environments (HPEs)), operate in conjunction with secure communications, systems integration software, and distributed software control information and support structures, to achieve the electronic contract/rights protection environment of the present invention. Together, these VDE components comprise a secure, virtual, distributed content and/or appliance control, auditing (and other administration), reporting, and payment environment. In some embodiments and where commercially acceptable, certain VDE participants, such as clearinghouses that normally maintain sufficiently physically secure non-VDE processing environments, may be allowed to employ HPEs rather VDE hardware elements and interoperate, for example, with VDE end-users and content providers."

- "VDE provides generalized configurability. This results, in part, from decomposition of generalized requirements for supporting electronic commerce and data security into a broad range of constituent "atomic" and higher level components (such as load modules, data elements, and methods) that may be variously aggregated together to form control methods for electronic commerce applications, commercial electronic agreements, and data security arrangements."

- "VDE provides a secure operating environment employing VDE foundation elements along with secure independently deliverable VDE components that enable electronic commerce models and relationships to develop."

- "VDE specifically supports the unfolding of distribution models in which content providers, over time, can expressly agree to, or allow, subsequent content providers and/or users to participate in shaping the control information for, and consequences of, use of electronic content and/or appliances. A very broad range of the functional attributes important for supporting simple to very complex electronic commerce and data security activities are supported by capabilities of the present invention. As a result, VDE supports most types of electronic information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements."

- "VDE supports a general purpose foundation for secure transaction management, including usage control, auditing, reporting, and/or payment. This general purpose foundation is called "VDE Functions" ("VDEFs"). VDE also supports a collection of "atomic" application elements (e.g., load modules) that can be selectively aggregated together to form various VDEF capabilities called control methods and which serve as VDEF applications and operating system functions."

- "VDE provides organization, community, and/or universe wide secure environments whose integrity is assured by processes securely controlled in VDE participant user installations (nodes)."

- "the end-to-end nature of VDE applications, in which content 108 flows in one direction, generating reports and bills 118 in the other, makes it possible to perform "back-end" consistency checks."

- "VDE can protect a collection of rights belonging to various parties having in rights in, or to, electronic information. This information may be at one location or dispersed across (and/or moving between) multiple locations. The information may pass through a "chain" of distributors and a "chain" of users. Usage information may also be reported through one or more "chains" of parties. In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed."

- "VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties. These parties may include content providers, electronic hardware manufacturers, financial service providers, or electronic "infrastructure" companies such as cable or telecommunications companies."

- "A rights application under VDE is made up of special purpose pieces, each of which can correspond to one or more basic electronic processes needed for a rights protection environment. These processes can be combined together like building blocks to create electronic agreements that can protect the rights, and may enforce fulfillment of the obligations, of electronic information users and providers. One or more providers of electronic information can easily combine selected building blocks to create a rights application that is unique to a specific content distribution model. A group of these pieces can represent the capabilities needed to fulfill the agreement(s) between users and providers. These pieces accommodate many requirements of electronic commerce including: the distribution of permissions to use electronic information; the persistence of the control information and sets of control information managing these permissions; configurable control set information that can be selected by users for use with such information; data security and usage auditing of electronic information; and a secure system for currency, compensation and debit management."

- "VDE allows electronic arrangements to be created involving two or more parties. These agreements can themselves comprise a collection of agreements between participants in a commercial value chain and/or a data security chain model for handling, auditing, reporting, and payment. It can provide efficient, reusable, modifiable, and consistent means for secure electronic content: distribution, usage control, usage payment, usage auditing, and usage reporting."

- "The features of VDE allow it to function as the first trusted electronic information control environment that can conform to, and support, the bulk of conventional electronic commerce and data security requirements. In particular, VDE enables the participants in a business value chain model to create an electronic version of traditional business agreement terms and conditions and further enables these participants to shape and evolve their electronic commerce models as they believe appropriate to their business requirements."

- "VDE provides the widely varying secure control and administration capabilities required for:

- 1. Different types of electronic content,
- 2. Differing electronic content delivery schemes,
- 3. Differing electronic content usage schemes,
- 4. Different content usage platforms, and
- 5. Differing content marketing and model strategies."

- "VDE controls auditing and reporting of electronic content and/or appliance usage."

- "VDE also securely supports the payment of money owed (including money owed for content and/or appliance usage) by one or more parties to one or more other parties, in the form of electronic credit and/or currency."

- "VDE can securely manage the integration of control information provided by two or more parties. As a result, VDE can construct an electronic agreement between VDE participants that represent a "negotiation" between, the control requirements of, two or more parties and enacts terms and conditions of a resulting agreement. VDE ensures the rights of each party to an electronic agreement regarding a wide range of electronic activities related to electronic information and/or appliance usage."

- "VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed finctionality. Furthermore, VDE permits participants to develop business models not feasible with non- electronic commerce, for example, involving detailed reporting of content usage information, large numbers of distinct transactions at hitherto infeasibly low price points, "pass-along" control information that is enforced without involvement or advance knowledge of the participants, etc."

- "VDE can support "real" commerce in an electronic form, that is the progressive creation of commercial relationships that form, over time, a network of interrelated agreements representing a value chain business model. This is achieved in part by enabling content control information to develop through the interaction of (negotiation between) securely created and independently submitted sets of content and/or appliance control information. Different sets of content and/or appliance control information can be submitted by different parties in an electronic business value chain enabled by the present invention. These parties create control information sets through the use of their respective VDE installations. Independently, securely deliverable, component based control information allows efficient interaction among control information sets supplied by different parties."

- "Employing VDE as a general purpose electronic transaction/distribution control system allows users to maintain a single transaction management control arrangement on each of their computers, networks, communication nodes, and/or other electronic appliances. Such a general purpose system can serve the needs of many electronic transaction management applications without requiring distinct, different installations for different purposes. As a result, users of VDE can avoid the confusion and expense and other inefficiencies of different, limited purpose transaction control applications for each different content and/or business model. For example, VDE allows content creators to use the same VDE foundation control arrangement for both content authoring and for licensing content from other content creators for inclusion into their products or for other use. Clearinghouses, distributors, content creators, and other VDE users can all interact, both with the applications running on their VDE installations, and with each other, in an entirely consistent manner, using and reusing (largely transparently) the same distributed tools, mechanisms, and consistent user interfaces, regardless of the type of VDE activity."

- "VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information."

- "VDE can further be used to enable commercially provided electronic content to be made available to users in user defined portions, rather than constraining the user to use portions of content that were "predetermined" by a content creator and/or other provider for billing purposes."

- "VDE supports a "universe wide" environment for electronic content delivery, broad dissemination, usage reporting, and usage related payment activities."

- "VDE provides important mechanisms for both enforcing commercial agreements and enabling the protection of privacy rights. VDE can securely deliver information from one party to another concerning the use of commercially distributed electronic content. Even if parties are separated by several "steps" in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered."

- "VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box, " a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means."

- "VDE supports multiple differing hierarchies of client organization control information wherein an organization client administrator distributes control information specifying the usage rights of departments, users, and/or projects."

- "Since VDE capabilities can be seamlessly integrated as extensions, additions, and/or modifications to fundamental capabilities of electronic appliances and host operating systems, VDE containers, content control information, and the VDE foundation will be able to work with many device types and these device types will be able to consistently and efficiently interpret and enforce VDE control information."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support, complete, modular separation of the control structures related to (1) content event triggering, (2) auditing, (3) budgeting (including specifying no right of use or unlimited right of use), (4) billing, and (5) user identity (VDE installation, client name, department, network, and/or user, etc.). ... Without such separation between these basic VDE capabilities, it would be more difficult to efficiently maintain separate metering, budgeting, identification, and/or billing activities which involve the same, differing (including overlapping), or entirely different, portions of content for metering, billing, budgeting, and user identification, for example, paying fees associated with usage of content, performing home banking, managing advertising services, etc. ... VDE modular separation of these basic capabilities supports the programming of plural, "arbitrary" relationships between one or differing content portions (and/or portion units) and budgeting, auditing, and/or billing control information."

- "A feature of VDE provided by the present invention is that certain one or more methods can be specified as required in order for a VDE installation and/or user to be able to use certain and/or all content."

- "A further feature of VDE provided by the present invention is that creators, distributors, and users of content can select from among a set of predefined methods (if available) to control container content usage and distribution functions and/or they may have the right to provide new customized methods to control at least certain usage functions (such "new" methods may be required to be certified for trustedness and interoperability to the VDE installation and/or for of a group of VDE applications)."

- "Each VDE participant in a VDE pathway of content control information may set methods for some or all of the content in a VDE container, so long as such control information does not conflict with senior control information already in place ...."

- "VDE supports commercially secure "extended" value chain electronic agreements. VDE can be configured to support the various underlying agreements between parties that comprise this extended agreement."

- "VDE agreements support evolving ("living") electronic agreement arrangements that can be modified by current and/or new participants through very simple to sophisticated "negotiations" between newly proposed content control information interacting with control information already in place ...."

- "All participants of VDE 100 have the innate ability to participate in any role."

- "any end-user may redistribute information received to other end-users."

- "Any VDE user 112 may assign the right to process information or perform services on their behalf to the extend allowed by senior control information."

- "As mentioned above, ROS 602 provides several layers of security to ensure the security of component assemblies 690. One important security layer involves ensuring that certain component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500."

- "An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network."

- "Moreover, when any new VDE object 300 arrives at an electronic appliance 600, the electronic appliance must "register" the object within object registry 450 so that it can be accessed."

- "The present inventions also provide for the use of a trusted third party electronic go-between or intermediary in various forms, including the "virtual presence" of such go-between through the rules and controls it contributes for distributed governance of transactions described in the present invention, and further through the use of a distributed, go-between system operating in on-line and/or off-line modes at various user and/or go-between sites. Such a trusted third-party go-between can provide enhanced and automated functionality, features and other advantages such as, for example .... These and other features and advantages provided by the present invention ..."

- "The Virtual Distribution Environment provides comprehensive overall systems, and wide arrays of methods, techniques, structures and arrangements, that enable secure, efficient electronic commerce and rights management on the Internet and other information superhighways and on internal corporate networks such as "Intranets". The present inventions use (and in some cases, build upon and enhances) this fundamental Virtual Distribution Environment technology to provide still additional flexibility, capabilities, features and advantages. The present invention, in its preferred embodiment, is intended to be used in combination a broad array of the features described in Ginter, et al, including any combination of the following:...."

- "parties using the Virtual Distribution Environment can participate in commerce and other transactions in accordance with a persistent set of rules they electronically define."

- "The present inventions preferred embodiment make use of a digital Virtual Distribution Environment (VDE) as a major portion of its operating foundation, providing unique, powerful capabilities instrumental to the development of secure, distributed transaction-based electronic commerce and digital content handling, distribution, processing, and usage management."

- "The Virtual Distribution Environment provides comprehensive overall systems, and wide arrays of methods, techniques, structures and arrangements, that enable secure, efficient electronic commerce and rights management on the Internet and other information superhighways and on internal corporate networks such as "Intranets". The present inventions use (and in some cases, build upon and enhances) this fundamental Virtual Distribution Environment technology to provide still additional flexibility, capabilities, features and advantages. The present invention, in its preferred embodiment, is intended to be used in combination a broad array of the features described in Ginter, et al, including any combination of the following: ..."

- "The Present Invention Solve These and Other Problems

As discussed above, a wide variety of techniques are currently being used to provide secure, trusted confidential delivery of documents and other items. Unfortunately, none of these previously existing mechanisms provide truly trusted, virtually instantaneous delivery on a cost-effective, convenient basis and none provide rights management and auditing through persistent, secure, digital information protection.

In contrast, the present inventions provide the trustedness, confidentiality and security of a personal trusted courier on a virtually instantaneous and highly cost-effective basis. They provide techniques, systems and methods that can being to any form of electronic communications (including, but not limited to Internet and internal company electronic mail) an extremely high degree of trustedness, confidence and security approaching or exceeding that provided by a trusted personal courier. They also provide a wide variety of benefits that flow from rights management and secure chain of handling and control."

- "The present inventions make use of these persistent electronic rules to provide secure, automated, cost-effective electronic control for electronic document and other digital item handling and/or delivery, and for the electronic formation and negotiation of legal contracts and other documents."

- "By way of non-exhaustive summary, these present inventions provide a highly secure and trusted item delivery and agreement execution services providing the following features and functions:

- Trustedness and security approaching or exceeding that of a personal trusted courier. ..
- Optional delayed delivery ("store and forward").
- Broadcasting to multiple parties. ...

- Trusted validation of item contents and delivery.
- Value Added Delivery and other features selectable by the sender and/or recipient.
- Provides electronic transmission trusted auditing and validating.
- Allows people to communicate quickly, securely, and confidentially.
- Communications can later be proved through reliable evidence of the communications transaction--providing non-repudiatable, certain, admissible proof that a particular communications transaction occurred.
- Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.
- Supports persistent rights and rules based document workflow management at recipient sites.
- System may operate on the Internet, on internal organization and/or corporate networks ("intranets" irrespective of whether they use or offer Internet services internally), private data networks and/or using any other form of electronic communications.
- System may operate in non-networked and/or intermittently networked environments.
- Legal contract execution can be performed in real time, with or without face to face or ear-to-ear personal interactions (such as audiovisual teleconferencing, automated electronic negotiations, or any combination of such interactions) for any number of distributed individuals and/or organizations using any mixture of interactions.
- The items delivered and/or processed may be any "object" in digital format, including, but not limited to, objects containing or representing data types such as text, images, video, linear motion pictures in digital format, sound recordings and other audio information, computer software, smart agents, multimedia, and/or objects any combination of two or more data types contained within or representing a single compound object.
- Content (executables for example) delivered with proof of delivery and/or execution or other use.
- Secure electronic containers can be delivered. The containers can maintain control, audit, receipt and other information and protection securely and persistently in association with one or more items.
- Trustedness provides non-repudiation for legal and other transactions.
- Can handle and send any digital information (for example, analog or digital information representing text, graphics, movies, animation, images, video, digital linear motion pictures,

sound and sound recordings, still images, software computer programs or program fragments, executables, data, and including multiple, independent pieces of text; sound clips, software for interpreting and presenting other elements of content, and anything else that is electronically representable).

- Provides automatic electronic mechanisms that associate transactions automatically with other transactions.
- System can automatically insert or embed a variety of visible or invisible "signatures" such as images of handwritten signatures, seals, and electronic "fingerprints" indicating who has "touched" (used or other interacted with in any monitorable manner) the item.
- System can affix visible seals on printed items such as documents for use both in encoding receipt and other receipt and/or usage related information and for establishing a visible presence and impact regarding the authenticity, and ease of checking the authenticity, of the item.
- Seals can indicate who originated, sent, received, previously received and redistributed, electronically view, and/or printed and/or otherwise used the item.
- Seals can encode digital signatures and validation information providing time, location, send and/or other information and/or providing means for item authentication and integrity check.
- Scanning and decoding of item seals can provide authenticity/integrity check of entire item(s) or part of an item (e.g., based on number of words, format, layout, image--picture and/or test--composition, etc.).
- Seals can be used to automatically associate electronic control sets for use in further item handling.
- System can hide additional information within the item using "stenanography" for later retrieval and analysis.
- Steganography can be used to encode electronic fingerprints and/or other information into an item to prevent deletion.
- Multiple steganographic storage of the same fingerprint information may be employed reflecting "more" public and "less" public modes so that a less restricted steganographic mode (different encryption algorithm, keys, and/or embedding techniques) can be used to assist easy recognition by an authorized party and a more private (confidential) mode may be readable by only a few parties (or only one party) and comprise of the less restricted mode may not affect the security of the more private mode.

- Items such as documents can be electronically, optically scanned at the sender's end--and printed out in original, printed form at the recipient's end.
- Document handlers and processors can integrate document scanning and delivery.
- Can be directly integrated into enterprise and Internet (and similar network) wide document workflow systems and applications.
- Secure, tamper-resistant electronic appliance, which may employ VDE SPUs, used to handle items at both sender and recipient ends.
- "Original" item(s) can automatically be destroyed at the sender's end and reconstituted at the recipient's end to prevent two originals from existing simultaneously.
- Secure, non-repudiable authentication of the identification of a recipient before delivery using any number of different authentication techniques including but not limited to biometric techniques (such as palm print scan, signature scan, voice scan, retina scan, iris scan, biometric fingerprint and/or handprint scan, and/or face profile) and/or presentation of a secure identity "token."
- Non-repudiation provided through secure authentication used to condition events (e.g., a signature is affixed onto a document only if the system securely authenticates the sender and her intention to agree to its contents).
- Variety of return receipt options including but not limited to a receipt indicating who opened a document, when, where, and the disposition of the document (stored, redistributed, copied, etc.). These receipts can later be used in legal proceedings and/or other contexts to prove item delivery, receipt and/or knowledge.
- Audit, receipt, and other information can be delivered independently from item delivery, and become securely associated with an item within a protected processing environment.
- Secure electronic controls can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be "destroyed" after a certain elapse of time or real time or after a certain number of handlings, etc.)
- Persistent secure electronic controls can continue to supervise item workflow even after it has been received and "read."
- Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility.

- Secure controls can be used in conjunction with digital electronic certificates certifying as to identity, class (age, organization membership, jurisdiction, etc.) of the sender and/or receiver and/or user of communicated information.

- Efficiently handles payment and electronic addressing arrangements through use of support and administrative services such as a Distributed Commerce Utility as more fully described in the copending Shear, et al. application.

- Compatible with use of smart cards, including, for example, VDE enabled smart cards, for secure personal identification and/or for payment.

- Transactions may be one or more component transactions of any distributed chain of handling and control process including Electronic Data Interchange (EDI) system, electronic trading system, document workflow sequence, and banking and other financial communication sequences, etc."

"All of these various coordination steps can be performed nearly simultaneously, efficiently, rapidly and with an extremely high degree of trustedness based on the user of electronic containers 302 and the secure communications, authentication, notarization and archiving techniques provided in accordance with the present inventions." The asserted claims also are invalid for violating the enablement and written description requirements to the extent that they are construed to recite subject matter that was not enabled by the application from which they issued, and/or not disclosed (e.g., the claims recite an element that was not disclosed in the written description, recite an element more broadly than was disclosed by the written description, recite subject matter for which there were no "blaze marks" in the written description pointing to such subject matter, combine elements from different embodiments that were not so combined in the written description, etc.) in that application. For example, at least the following bold-faced claim language was not so enabled and/or disclosed, at least not as the claims apparently are being "construed" by InterTrust to attempt to support its untenable infringement allegations:

'193

1) A method comprising:

a) receiving a digital file including music;

b) **storing said digital file in a first secure memory of a first device;**

c) **storing information associated with said digital file in a secure database stored on said first device, said information including at least one budget control and at least one copy control, said at least one budget control including a budget specifying the number of copies**

which can be made of said digital file; and said at least one copy control controlling the copies made of said digital file;

d) determining whether said digital file may be copied and stored on a second device based on at least said copy control;

e) if said copy control allows at least a portion of said digital file to be copied and stored on a second device,

f) copying at least a portion of said digital file;

g) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

h) storing said digital file in said memory of said second device; and

i) including playing said music through said audio output.

2) A method as in claim 1, further comprising:

a) at a time substantially contemporaneous with said transferring step, recording in said first device information indicating that said transfer has occurred.

3) A method as in claim 2, in which:

a) said information indicating that said transfer has occurred includes an encumbrance on said budget.

4) A method as in claim 3, in which:

a) said encumbrance operates to reduce the number of copies of said digital file authorized by said budget.

11) A method comprising:

a) receiving a digital file;

b) storing said digital file in a first secure memory of a first device;

c) storing information associated with said digital file in a secure database stored on said first device, said information including a first control;

d) determining whether said digital file may be copied and stored on a second device based on said first control, said determining step including identifying said second device and determining whether said first control allows transfer of said copied file to said second

device, said determination based at least in part on the features present at the device to which said copied file is to be transferred;

e) if said first control allows at least a portion of said digital file to be copied and stored on a second device,

f) copying at least a portion of said digital file;

g) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

h) storing said digital file in said memory of said second device; and

i) rendering said digital file through said output.

15) A method comprising:

a) receiving a digital file;

b) an authentication step comprising:

c) accessing at least one identifier associated with a first device or with a user of said first device; and

d) determining whether said identifier is associated with a device and/or user authorized to store said digital file;

e) storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;

f) storing information associated with said digital file in a secure database stored on said first device, said information including at least one control;

g) determining whether said digital file may be copied and stored on a second device based on said at least one control;

h) if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,

i) copying at least a portion of said digital file;

j) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

k) storing said digital file in said memory of said second device; and

l) rendering said digital file through said output.

19) A method comprising:

a) receiving a digital file at a first device;

b) establishing communication between said first device and a clearinghouse located at a location remote from said first device;

c) said first device obtaining authorization information including a key from said clearinghouse;

d) said first device using said authorization information to gain access to or make at least one use of said first digital file, including using said key to decrypt at least a portion of said first digital file; and

e) receiving a first control from said clearinghouse at said first device;

f) storing said first digital file in a memory of said first device;

g) using said first control to determine whether said first digital file may be copied and stored on a second device;

h) if said first control allows at least a portion of said first digital file to be copied and stored on a second device,

i) copying at least a portion of said first digital file;

j) transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output;

k) storing said first digital file portion in said memory of said second device; and

l) rendering said first digital file portion through said output.

<u>'683</u>

2. A system including:

a first apparatus including,

user controls,

a communications port,

a processor,

a memory storing:

a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;

a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule, the first secure container rule having been received from a third apparatus different from said second apparatus; and

hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;

a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said **protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container**; and

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

28. A system including;

a first apparatus including;

user controls,

a communications port,

a processor,

a memory containing a first **rule,**

hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;

a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus**, said **protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and a second apparatus including:

user controls,

a communications port,

a processor,

a memory containing a second **rule,**

hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;

a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said **protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;**

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and

an electronic intermediary, said intermediary including a user rights authority clearinghouse.

29. A system as in claim 28, said **user rights authority clearinghouse operatively connected to make rights available to users.**

<u>PLR 3-4 Production</u>

Each reference identified pursuant to PLR 3-3(a) but not in the prosecution history, and the documents referenced in PLR 3-4 that are sufficient to show the operation of the accused features of the products specifically identified in InterTrust's PLR 3-1 Statements of October 29 and November 5, 2001, and "Addendum" dated March 12, 2002, has been or is being produced, or is otherwise available for inspection and copying.

Dated: August 16, 2002

By: ____
WILLIAM L. ANTHONY, State Bar No. 106908
ERIC L. WESENBERG, State Bar No. 139696

HEIDI L. KEEFE, State Bar No. 178960
MARK R. WEINSTEIN, State Bar No. 193043
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
MICROSOFT CORPORATION

Of Counsel:

T. Andrew Culbert, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

DECLARATION OF SERVICE BY MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 121 S.W. Salmon St., Portland, Oregon 97204

On August 16, 2002, I served:

MICROSOFT'S PRELIMINARY INVALIDITY CONTENTIONS REGARDING U.S. PATENTS 6,253,193 & 6,185,683 PURSUANT TO PLR 3-3, 3-4

by e-mail and by placing true copies of these papers in each of separate envelopes addressed to:

Michael Page, Esq. KEKER & VAN NEST, LLP 710 Sansome Street San Francisco, CA 94111 mhp@kvn.com	Steven H. Morrissett, Esq. Finnegan Henderson Farabow Garrett & Dunner Stanford Research Park 700 Hansen Way Palo Alto CA 94304-1016 steven.morrissett@finnegan.com
	Stephen E. Taylor, Esq. Taylor &Co. Law Offices 1050 Marina Village Parkway Suite 101 Alameda, CA 94501 staylor@tcolaw.com

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Portland, Oregon.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 16, 2002, at Portland, Oregon.

____
(SIGNATURE)

____
(PRINT NAME)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

MICROSOFT PLR 3-3(c) CHARTS

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
2. A system including:		Reference is made to (1) each Stefik reference cited in the asserted InterTrust patents, and to USP 5,715,403; (2) all related methods practiced at Xerox PARC and/or ContentGuard prior to InterTrust's alleged priority date	Reference is made to Proceedings, Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project, v. 1 no. 1 (Jan 1994) ("CNI/IMA 94"), and its 1993 proceedings in Cambridge, MA	Reference is made to "Copyright Protection for Electronic Publishing over Computer Networks," A.K. Choudhury, N.F. Maxemchuk, S. Paul, H.G. Sculzrinne.	Reference is made to Tygar & Yee, "Strongbox: A System for Self-Securing Programs" in CMU Computer Science: A 25th Anniversary Commemorative, R. Rashid, ed. (ACM Press 1991) ("SB"); "Cryptography: It's Not Just for E-mail Anymore," (Tech. Report CMU-CS-93-107, Carnegie Mellon Unic. March 1993) ("ES"); and/or "Dyad: A System for Using Physically Secure Coprocessors." (Carnegie Mellon Univ., CMU-CS-91-140R, May 4, 1991) (see also CNI/IMA 94). Dyad refers to and supplements the Strongbox and ES references; SB comprises a loosely coupled network of machines with different security levels, using key exchange, secure processors and memory, authentication and capabilities, finger printing, and verified boot
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	E.g., a computer. See, e.g., USP 5,715,403; USP 5,634,012.	A computer. See, e.g., R. J. Linn, "Copyright and Information Services in the Context of the National Research and Education Network" and references to it; Robert E. Kahn, "Deposit, Registration and Recordation in an Electronic Copyright Management System" ("Kahn"); J.D. Tygar and Bennet Yee, "Dyad: A System for Using Physically Secure Coprocessors" ("Dyad"); see also, e.g., Cupid, KALA, and Griswold articles	First apparatus could be any "client" or user computer, or any document or copyright server. See e.g. Figs. 1 & 2.	ES: any first user's "apparatus," e.g. a computer); electric postage meter (EPM); printer; Post Office computer; SB: any first "apparatus"
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	"apparatus" has user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	one or more comm. ports
(3) a processor,	Consumer's computer, as shown	See 2(a)	See 2(a)	See 2(a)	a processor

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
	in WMRM SDK				
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	and a memory storing:
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	Secure container (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")	"secure container" is indefinite, but as used by InterTrust in its 3-1 Statement would include the digital works described in Stefik, and/or (or such as) digital certificates or authorizations. Systems or components (including digital works) may be object-oriented.[1]	"secure container" and "item" are indefinite, but as used by InterTrust in its 3-1 Statement appear to include, for example, any file having any aspect of "security." Such an "item" may be a message or literary or instructional text, for example. Part or all of such "items" may be encrypted; it would also be obvious that one could do so. Note also that in Linn, Kala, Dyad et al., systems and/or components may be object-oriented. By InterTrust's allegations, additional examples of "secure containers" in e.g. Dyad could be the secure coprocessor and/or its associated software, a contract or contract template, a partly or wholly encrypted program, electronic currency, or smart cards.	By InterTrust's construction, any file received from any 2nd apparatus (e.g. floppy or download, e.g. from the "document server") any part of which is "encrypted"	ES: stamp (currency) is received from provider (EPM) and stored on user apparatus SB: any self-securing program(s) or other encrypted information
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	"Rule" is indefinite, but as used by InterTrust in its 3-1 Statement this element would include certificates and other digital works that move between repositories subject to usage rights (and which can come from a 3d source)	numerous so-called "rules" may be received from any third apparatus, such as right to render or copy. See, e.g., Linn, Kahn (EBR, terms and conditions on use, usage restrictions and/or payment requirements), Dyad (bindings, 3rd party instructions, contracts, contract bindings, additional contracts, secure coprocessor-supported requirements, other secure coprocessors and/or associated hardware or software, and upgrades or further upgrades)	satisfying copyright server's authentication request(s) (e.g. through permission, signature, authentication, access controls (persona, anonymous, user)), name and password, access control lists, capabilities, shared secrets, challenge-response, encryption (public key and/or symmetrical), key certificate techniques, Kerberos	ES: any currency "rule" received from 3d apparatus (e.g., permission from root, or passphrase from keyboard or other apparatus); rights portion from EPM SB: any partly or wholly encrypted information from any White Pages server, and/or fingerprinted data or program files
(5) hardware or software used for receiving and opening secure	Windows Media Player and Windows Media Rights	system hardware or software	system hardware or software	client and server hardware or software	ES: EPM and associated hardware or software

[1] It was obvious to use any known techniques as in e.g. Smalltalk, Bento and/or OLE/COM in connection with disclosures of Stefik, CNI/IMA 94, Choudhury/Maxemchuk, Tygar/Yee, Blaze, etc. See, for example, W. LaLonde, J. Pugh, Inside Smalltalk (Prentice Hall 1990); Harris et al., Apple Bento, Specification v 1.0d5 (July 1993); Peter Coad, "Object Oriented Patterns" (Comm. of the ACM, Sept. 1992); OLE 2 Programmers Reference vol. 1 (Microsoft Press 1994). For example, using the observer design pattern or model view controller or broadcast pattern, objects can initiate notifications regarding embedded objects, e.g., objects may be saved to secure data stream and transferred to other controls. Another example is the COM Service Control Manager.

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Manager				SB: e.g. SB, Mach, Camelot, secure processor
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	" and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	e.g. protected repositories, certificates, usage rights, and associated systems and software	describes numerous examples of what InterTrust appears to consider "protected processing environments" where "rules" are applied	1st and 2nd "rules" consist of any 2 valid "rules" referenced above; alleged "PPE" includes protected client and server processes	ES: 1st and 2nd "rules" consist of any two valid "rules" specified above; "PPE" as alleged would include the application and OS processes for protecting operation of the system SB: "secure" loader (second server), and/or any user-supplied access-control/authorization system (167)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	hardware or software used for transmission	hardware or software used for transmission	system hardware or software (see e.g. Figs. 1-2)	ES: any hardware or software employed in transmitting currency SB: see 2(a)(4)(i); any system hardware or software employed in transmission
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	any user apparatus (e.g. P.C.) with: See 2(a)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	client or server apparatus	user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	client or server apparatus	a communications port
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	client or server apparatus	a processor, and
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right received as part of a signed license (WMRM SDK, Step9)	See 2(a)	See 2(a)	client or server apparatus	a memory containing a "first rule"
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or	See 2(a)(5)	See 2(a)(5)	client or server apparatus	ES: EPM and associated hardware and software SB: See 2(a)(5)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
being associated with each of said secure containers;	rules via Windows Media Player and Windows Media Rights Manager.				
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	See 2(a)(6)	process environment protected from tampering; "rules" applied to govern access or use of file contents	protected client and server processes apply "rules" according to InterTrust	see 2(a)(6)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)
(b) a second apparatus including:	2nd consumer's computer	See 2(a)	2nd client or server apparatus	2nd user apparatus	2nd user apparatus
(1) user controls,	2nd consumer's computer	See 2(a)	See 28(b)	2nd user apparatus	2nd user apparatus
(2) a communications port,	2nd consumer's computer	See 2(a)	See 28(b)	2nd user apparatus	2nd user apparatus
(3) a processor,	2nd consumer's computer	See 2(a)	See 28(b)	2nd user apparatus	2nd user apparatus
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	Memory in a repository or other user apparatus; usage rights and/or security levels supply "rules"	memory in 2nd apparatus contains "second rule" according to InterTrust	memory in 2nd apparatus contains "second rule" according to InterTrust	2nd user apparatus
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 28(a)(5)	see 28(a)(5)	2nd user's apparatus; "secure container rule or rules" applied via e.g. OS (e.g. Mach, Unix) and/or file systems like CFS or Andrew. See also 28(a)(5)	2nd user's apparatus; "secure container rule or rules" applied via e.g. OS (e.g. Mach, Unix) and/or file systems like CFS or Andrew. See also 28(a)(5)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media	see 28(a)(6)	see 28(a)(6)	see 28(a)(6)	see 28(a)(6)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Rights Manager; processing environment applies multiple rules in combination				
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 28(a)(7)	see 28(a)(7)	see 28(a)(7)	see 28(a)(7)
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	Credit server or any (other) "intermediary" repositories for user or usage rights or capabilities	Linn - copyright server or other "intermediary"/"rights-issuer" connected to other users of system; Kahn – RMS, RRS, and/or repositories; Dyad – any machine or system (such as a distributor or contractor) serving alleged "clearinghouse" function	copyright server	ES: local P.O. (or EPM with multiple users) SB: White Pages server
29. A system as in claim 28.					
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	28(c) above, "operatively connected" to user(s)	28(c) above, "operatively connected" to user(s)	28(c) above, "operatively connected" to user(s)	ES: local or other P.O. (or EPM with multiple users) "operatively connected" to make rights available to users SB: White Pages server

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust) - continued

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
2. A system including:		Reference is made to B. Clifford Neuman, "Proxy-Based Authorization and Accounting for Distributed Systems," Proceedings of the 13th Int'l Conf. on Distributed Computing Systems, May 1993; see also www.isi.edu/people/bcn/publications.html	Reference is made to D. W. Davies, W. L. Price, Security for Computer Networks (John Wiley & Sons 1989) See, for example, Chapter 6, "Key Management"; see also the description of ATMs, EFT & POS systems (e.g., pp. 297-339); reference is also made to the public knowledge, use, and sale of such systems in the U.S. prior to 2/13/94; see also S. Muftic, Security Mechanisms for Computer Networks (Halstead Press, a div. of John Wiley & Sons, 1984) re authentication cards	Reference is made to David Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. of the ACM, vol. 28 no. 10, Oct. 1985; see also "Wallet Databases with Observers," Advances in Cryptology-Proceedings of Crypto '92 (pp. 89-105; "Achieving Electronic Privacy," (Scientific American 1992); www.chaum.com/articles/list_of_articles.htm	Reference is made to each of RSA Data Security Conference 1/12-14/94 (re Telescript, RSA, General Magic); USP 5,603,031; USP 6,016,393; and White, J.E., Telescript Technology: The Foundation for the Electronic Marketplace (1994). On information and belief, Telescript was also used in AT&T PersonaLink before 2/13/95.	Reference is made to each of Custer, Inside NT (Microsoft Press 1993) and NT software, including NT security levels and/or NT in combination with Kerberos or other certificate, signature or other encryption methods (e.g., Kerberos API routed through NT security subsystem). See e.g. Custer at 26-31, 329-30.	This claim as asserted is also anticipated by a simple Bell-LaPadula model, widely known in the U.S. before 2/13/94 -- see, e.g., discussion in Castano et al., Database Security (Addison Wesley 1994)
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	e.g. client c in Fig. 3	any computer in a network, e.g. terminal 2 in Figure 6.3, or an ATM machine or bank computer (e.g. in shared ATM systems)	any first computer, e.g. a personal card computer	a first computer having	a first PC (client or server)	Apparatus 1 could also be a filesystem computer
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	has user controls	user controls	has user controls	has user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a comm port	a comm port	a comm port	a comm port
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a processor	a processor	a processor	a processor

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	See 2(a)	memory stores:	and a memory	and a memory	and a memory	and a memory
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	Secure container (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")	so-called "secure container" as alleged by InterTrust would cover Kerberos tickets which may be received from a server, e.g. for a read capability. Alternatively, any partly encrypted file.	encrypted files, messages, session keys and terminal keys; ATM card or wholly or partly encrypted instructions or data received from bank computer (e.g., balance)	One or more enabling credentials or "container" thereof	a first agent (object), or associated file, encrypted in whole or part, received from a 2d "apparatus."	File with any "item" "at least in part encrypted" received from a second "apparatus" – e.g., a cryptographically signed and/or sealed or otherwise at least partly encrypted file received from another computer	a second apparatus operating at a particular security level may develop information (an object) classified at a particular security level, and store it at apparatus 1
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	so-called "rule" received from e.g. server or end server, or knowledge about the authorization received from another source; capabilities may be revocable and have expiration times; access control lists support compound principal identifiers	"rule" of any transaction, or PIN or watermark and/or user ID from card; "rights portion" of data sent from key distribution server	applying any "rule" obtained from a "shop" or "rule" for exposing credit info	a permit from a 3d apparatus (e.g. associated with a 2d agent meeting a 1st)	InterTrust's 3-1 Statement uses "rule" in so general a sense that it could be any password, key, ticket, permission, clearance, right, capability, or access control used in NT (see (6) below)	when a third apparatus seeks access to stored object, it must provide security level information (e.g. a security label)
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	passim; possible "rules" include for-use-by-group, accept-once, quota, authorized, limit-restriction	system hardware or software for opening files, messages, deciphering session keys; ATM receives cards having keys or other "governed" data; receives data from bank computers	system hardware or software, e.g. to process credentials	system hardware or software, e.g. engine	system hardware or software	system hardware or software (e.g., Apparatus 1 applies BLP rules, which determines whether the third apparatus is granted access or not. Permissions include but are not limited to write, read, copy, execute).
(6) a protected processing environment at least in part protecting information contained in said protected	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights	"rules" as asserted by InterTrust may be any of multiple (e.g.	second "rule" could be, e.g., balance information, account limits, or any other	processing has safeguards; "rules" allow electronic commerce of varying	processing has safeguards; "rules" as InterTrust alleges the term would cover permits	"1st and 2nd rules" as alleged by InterTrust could consist of any 1 or more of	processing has safeguards; see, e.g. (5) re BLP rules. It would also be obvious to

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	cascaded) proxies; any accounting rules; any policy programming steps; and any underlying access controls or other authorization or authentication. See also Kerberos	contractual rule or access requirement; use of session key and terminal key to decipher a file/message, see e.g. Figure 6.3; using the keys to authenticate the terminals; applying authentication and decipherment to open files/messages	characteristics	and intersections as well as meeting results, in service of policies or any transaction calculus	the features which protect information in NT, including access controls, security subsystem, security reference monitor and passwords, login, Kerberos, enforces security policies, guards operating system resources, and performs run-time object protection and auditing; see also data shielding and integrity functions, e.g. in communications, computing, and databases.	use any of the cumulative protections described in the accompanying document under Suggestions to combine and motivations to combine.
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	hardware or software employed in transmitting tickets	any hardware and software use to transmit files/messages between terminals; e.g. ATMs and the rest of the associated banking system	personal card computer has transmission capabilities	hardware or software is used for transmission	any hardware or software employed in transmitting files or tickets	hardware or software is used for transmission
28. A system including:	▨	▨	▨	▨	▨	▨	▨
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(4) a memory containing a first rule,	Memory is in the consumer's computer,	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
	first rule is a right received as part of a signed license (WMRM SDK, Step9)						
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
(b) a second apparatus including:	2nd consumer's computer	any 2d computer	any 2d computer (e.g., of terminals 1, 2); a 2d ATM or bank computer	any 2d card or other device	any 2d computer	Any second computer, e.g. server or client computer running NT	any second user's computer
(1) user controls,	2nd consumer's . computer	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)
(2) a communications port,	2nd consumer's computer	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)
(3) a processor,	2nd consumer's computer	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules in combination	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
use of a governed item;							
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	e.g. group server, end server, authorization server, or any remote server	key distribution center; bank "clearinghouse"	credential "clearinghouse"	any server or other machine playing "intermediate" role with "clearinghouse" function, e.g. with permits or keys	NT server in any "clearinghouse" role, e.g. admin or host; see also Kerberos	server in any "clearinghouse" role
29. A system as in claim 28,							
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	system of 28(c)	system of 28(c)	system of 28(c)	system of 28(c)	system of 28(c)	system of 28(c)

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust) - continued

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
2. A system including:		"CUPID" is described in e.g. "Protocols and Services (Version 1): An Architectural Overview" (November 1992) (CUPID Architecture Subcommittee); see also CNI/IMA 94	Reference is made to each of Blaze, "A Cryptographic File System for Unix" (First ACM Conference on Communications and Security, 1993) (and preprint); "Key Management in an Encrypting File System" (Usenix 1994); and (with John Ioannidis) "The Architecture and Implementation of Network – Layer Security Under Unix" (Proceedings of 1994 Winter	Reference is made to ORION/ITASCA and Thor secure object oriented database systems, and to the work of Martin S. Olivier in the development of SECDB, 1990-1995, at Rand Afrikaans University, South Africa. See Olivier, M., et al, "Building a Secure Database using Self-Protecting Objects," Computers & Security, Vol. 11, No. 3, 1992; Olivier, M., et al, "DISCO: A	Reference is made to J. Kohl, C. Neuman, RFC 1510, "The Kerberos Network Authentication Service (V5)"; see also descriptions of, references to and suggested combinations with Kerberos in, e.g., Davies, Neuman, Custer; see also, generally, MIT's Project Athena and secure authenticated e-mail, e.g. RFCs 1154-55

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
			USENIX Conference Proceedings, 1994)	Discretionary Security Model for Object-oriented Databases" in G.G. Gable and W.J. Caelli (eds.), IT Security: The Need for International Cooperation, 345-357 (Elsevier 1992); Olivier, M., et al, "A Taxonomy for Secure Object-Oriented Databases," ACM Transactions on Database Systems, Vol. 19, No. 1, 1994; Olivier, M., "Secure Object Oriented Databases," Doctoral Thesis, December 1991, Rand Afrikaans University.	
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop[2]	any user apparatus (e.g., a host machine or client PC)	any computer in the distributed network	First apparatus is recipient's (Bob) computer.
(1) user controls,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	any computer in the distributed network	User controls of recipient computer.
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	any computer in the distributed network	Communications ports of recipient computer.
(3) a processor,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	Any computer in the distributed network	Processor of recipient computer.
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	Any computer in the distributed network	Memory of recipient computer.
(i) a first secure containeScontaining a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	ainer (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains. encrypted governed item ("Encrypted content")	Secure/ Encrypted copy of Printjob, or Printjob Order, or content file received by Printshop from Orgination Server, Reference Server or Gatekeeper Server, having been packaged directly by or referenced (via subdocument fields within a Printjob) by the Publisher's CUPID Client.	Scenario 1 – CFS files are received from other accounts or users or by download or from floppy (e.g., content providers) Scenario 2 – any "secure" file received from sender with credential saved in another group's directory	SOODB objects could be "secure containers" as alleged by InterTrust; "governed item" may be internal data type or external by reference. Object is instantiated from remote system where it persists.	"First secure container" is transmission (datastream or file) sent from sender Alice's computer (the "second apparatus") to recipient Bob's computer. The transmission includes a message (the "governed item") sent by Alice to Bob, which is encrypted with the (shared secret) session key K_{AB}.

[2] The CUPID Architecture defines two kinds of Servers: *Origination Servers* and *Notification Servers*. These terms refer both to the software (in UNIX terms, the daemons) that provides the specified services and to the computers upon which this software is running. A single computer may operate as both an Origination Server and a Notification Server. CUPID allows Printshop systems to be organized in a variety of ways. A single program, for example, might perform all the Printshop's CUPID Client functions and also act as the printer server. Alternatively, several programs running on several computers might act as specialized CUPID Clients, communicating with a printer server running on yet another host.

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	**Scenario 1:** Contained within a Printjob, or Printjob Order are Tasks, Operation Specifications and Pre-requisite Task Lists, each contains rules, tasks, or instructions that must be followed in order to reproduce the content file.[3] **Scenario 2:** The Printshop Client, Notification Server, or any Agents running on the Printshop Server, can access and	"rule" as alleged by InterTrust could be any of: - key received from an apparatus other than the apparatus the file came from (e.g., from root or an admin account) - smart card key(s) rcvd from smart card; - passphrase rcvd from keyboard and/or other input apparatuses	Secure container "rule" is received from third system where the class for the remote object is persisted. "Rule" implements some control over access to object, such as multi-level security or method authorization	"First secure container rule" is any of four values (sender and recipient IDs, a time stamp (TS), a time duration (TD)) in the recipient ticket originating from the Kerberos server (aka, key distribution center or KDC), and forwarded to the recipient computer (first apparatus) from the sender computer (second apparatus). The recipient ticket includes: sender and recipient IDs, a time stamp (TS), a time duration (TD), and the session

[3] Anatomy of a Printjob, including Printjob Order:

Printjob Header ***(which includes)***
Publisher ID;
Date and time submitted;
Job Name, used for Publisher identification purposes, not necessarily the same as the Document title;
Job Limits (optional), used to extend or reduce the default Printjob retention period on the Origination Server;
Security Keys (if and as required);
General free-text comments, intended to be seen by all Parties working on this Printjob.
[Subdocument File(s)]
Status* (includes Status of all Printjob elements)
Message Queue*
..... and 1 or more Printjob Order(s)
Printjob Order Header ***(which includes)***
Printshop ID;
Order Name (used for Publisher identification purposes);
Scheduling, priority, and/or deadline information;
Authorization codes, if any (i.e., authorization codes defined and known by the Publisher and the Printshop *outside* of CUPID, by virtue of separate contractual or other arrangements); and
General free-text comments (intended to be seen by all Parties working on this Order).
[Complete Document]
Task(s)
Operation
[Object]
[Opspecs]
[Agent]
[Prerequisite Task List]

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
		download their specific tasks from the Origination Server Message Queue. These messages contain instructions that must be followed in order to reproduce the content file. **Scenario 3:** Cupid Agents may be used to govern aspects of access on use. Agents may be employed by Publishers, Printshops, or other Agents	Also in Scenario 2 – verifying credentials of sender		key K_{AB}. The IDs, TS and TD together govern use of the session key to access (decrypt) the sender's message (governed item) at the recipient computer. For example, Kerberos protocol limits use of the session key to the time period specified by TS, TD, and limits the message exchange to the principals specified by IDs.
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	The Printshop CUPID Client is responsible for receiving content files, from any source, and messages from the Origination Server Message Queue.[4]	associated networked hardware and software	SOODB process and/or object methods	Network adapter, networking protocol software, Kerberos protocol software or hardware, and decryption software (e.g., DES decryptor) are used to receive and open the sender's message on the recipient computer.
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	The UNIX Server running at the Printshop protected from physical access or by UserID & Password. Access to content can be protected by predetermined keys stored in the Printjob Header. The Printshop CUPID Client accesses and renders the content. Caching of text, images, or other information at locations other than the Origination Server may be invisible to Clients and complies with CUPID's security provisions. The CUPID Client also ensures that any tasks or instructions are carried out according to the Message Queue,	any two valid "rules" referenced above; or 2d rule could also be logon, or Unix permission (user/group/world, read/write/execute); "PPE" may include CFS and/or Unix processes for protecting operation of system; in scenario 2, whether sender can write to designated file	the trusted architecture implementing the SOODB framework. "Second rule" as InterTrust would have it can include any identification/authorization	"Second secure container rule" is any of the other three of the four values in the recipient ticket. Note that the sender and recipient IDs in the recipient ticket actually originates from the initial ticket request from the sender computer to the KDC server. All four values in the recipient ticket are applied in combination to govern use of the session key to access (decrypt) the sender's message. "PPE" is the Kerberos protocol software on the recipient computer.

[4] In CUPID, the Message Queue may reside on the Origination Server for that Printjob, and accumulate Messages related to the Printjob that are targeted for the Publisher, the Printshop, and any Agents referenced by the Printjob. A Client connecting to a Server may request the accumulated messages for the appropriate Publisher, Printshop, or Agent. [Publishers, Printshops, and Agents may be notified via electronic mail [secured by encryption or obvious to do so] that one or more CUPID messages are waiting.]

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
		Pre-requisite Task List, or Tasks contained in the Printjob Order.[5]			
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	CUPID Client can either communicate directly with printer devices, or can communicate with Printer Servers for spooling and queuing of work. Subdocument Files, may be defined to be (optionally) pointers to Subdocuments, rather than the actual contents of the Subdocuments. These pointers might refer to files outside of CUPID, and may include keys or other access-control information	any hardware or software employed in transmitting files	any hardware or software allowing interconnection and intercommunication in the distributed SOODB	Recipient computer's network card and networking protocol software.
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	any user apparatus (e.g. host machine or client P.C.)	Any computer in the distributed network	First apparatus is sender's (Alice) computer.
(1) user controls,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	See 2(a)	Any computer in the distributed network	User controls of sender computer.
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	See 2(a)	Any computer in the distributed network	Communications ports of sender computer.
(3) a processor,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	See 2(a)	Any computer in the distributed network	Processor of sender computer.
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right received as part of a signed license (WMRM SDK, Step9)	UNIX Server running at a Printshop	any of: -any key or permission in memory; -smart card key(s) rcvd from	Memory of a computer in the distributed network, storing the caller's capability (i.e. non-forgeable token) for example	Memory of recipient computer. "First secure container rule" is any of four values (sender and recipient IDs, a time stamp (TS), a time duration

[5] CUPID provides inter alia: (a) the network delivery of print-ready electronic documents; (b) the authorization of *who* is to print or distribute finished documents; (c) the communication of information as to *how* the document are to be printed and distributed, including steps of proofing and estimating; (d) the support of business functions, such as payment for printing services and specification and collection of royalties or other fees; (e) support for security; (f) conversion of document formats; and (g) CUPID protocols and services that support these functions.

The CUPID architecture further comprises/features:

- Internet-based utility that provides services to enable distributed printing;
- Protocol to send document over network, with job instructions and status information;
- Initial distributed services include: access control; authentication; encryption/decryption; images text conversion; routing; assembly; job status and resource tracking;
- Pointers to remote stored documents; end-user desktop assembly of custom documents; print-time merge of component materials; print-time final edit; etc.

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
			smartcard; -passphrase rcvd from keyboard or other input apparatus; -or other access limitations (such as credentials or logon), or managed resources (such as budgeted CPU time or memory)		(TD)) in the sender ticket returned from the Kerberos server (aka, key distribution center or KDC) in response to sender computer's ticket request. Sender ticket includes: sender and recipient IDs, a time stamp (TS), a time duration (TD), and the session key K_{AB}. The IDs, TS and TD together govern use of the session key to access (decrypt) a response message (governed item) from the recipient computer. For example, Kerberos protocol limits use of the session key to the time period specified by TS, TD, and limits the message exchange to the principals specified by IDs.
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	Printshop CUPID Client is responsible for receiving content files from any source, and messages from the Origination Server Message Queue.	user can use hardware or software to receive and "open" wholly or partially encrypted files	The above computer and/or associated processes. SOODB objects could be "secure containers" as alleged by InterTrust. "Governed item" may be internal data type or external by reference	"Secure container" is transmission (datastream or file) sent from recipient computer (the "second apparatus") to sender computer. The transmission includes a response message (the "governed item") sent by Bob to Alice, which is encrypted with the (shared secret) session key K_{AB}. Network adapter, networking protocol software, Kerberos protocol software or hardware, and decryption software (e.g., DES decryptor) are used to receive and open Bob's message on the sender computer.
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	UNIX Server running at the Printshop is protected from physical access and by UserID & Password. Access to content can be protected by predetermined keys stored in the Printjob Header. CUPID Client ensures that tasks and instructions are carried out according to the	As construed by InterTrust, "1st rule" and "a secure container rule" could be any two valid "rules" referenced above; "PPE" includes file and operating system processes for protecting system operation	SOODB process and/or object methods in the trusted computing base. "Secure container rule" is received from third system where the class for the remote object is persisted. "Rule" implements some control over access to object, such as multi-level security or method authorization	"secure container rule" is any of the other three of the four values in the recipient ticket. Note that the sender and recipient IDs in the recipient ticket actually originates from the initial ticket request from the sender computer to the KDC server. All four values in the recipient ticket are applied in combination to govern use

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
		Message Queue, Pre-requisite Task List, and/or Tasks contained in the Printjob Order.			of the session key to access (decrypt) Bob's message. "PPE" is the Kerberos protocol software on the recipient computer
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	CUPID Client can communicate with Printer Servers, displays or printer devices	any hardware or software employed in transmitting wholly or partly encrypted files	Any hardware or software allowing interconnection and intercommunication in the distributed SOODB	Sender computer's network card and networking protocol software.
(b) a second apparatus including:	2^{nd} consumer's computer	2^{nd} apparatus, e.g. 2nd Unix Server running at a Printshop	2^{nd} user's apparatus	The trusted architecture implementing the SOODB framework. "Second rule" is subject identification/authorization	First apparatus is recipient's (Bob) computer.
(1) user controls,	2^{nd} consumer's computer	2^{nd} apparatus	2^{nd} user apparatus	2^{nd} apparatus	User controls of recipient computer.
(2) a communications port,	2^{nd} consumer's computer	2^{nd} apparatus	2^{nd} user apparatus	2^{nd} apparatus	Communications port of recipient computer.
(3) a processor,	2^{nd} consumer's computer	2^{nd} apparatus	2^{nd} user apparatus	2^{nd} apparatus	Processor of recipient computer.
(4) a memory containing a second rule,	Memory is in 2^{nd} consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	memory in 2^{nd} apparatus contains "second rule" according to InterTrust	memory in 2^{nd} apparatus contains "second rule" according to InterTrust	memory in 2^{nd} apparatus contains "second rule" – a classification level of the class for example	Memory of recipient computer. "Second rule" is any of four values (sender and recipient IDs, a time stamp (TS), a time duration (TD)) in the recipient ticket originating from the Kerberos server (aka, key distribution center or KDC), and forwarded by sender computer to recipient computer. Recipient ticket includes: sender and recipient IDs, a time stamp (TS), a time duration (TD), and the session key K_{AB}. The IDs, TS and TD together govern use of the session key to access (decrypt) a message (governed item) from the sender computer. For example, Kerberos protocol limits use of the session key to the time period specified by TS, TD, and limits the message exchange to the principals specified by IDs.
(5) hardware or software used for receiving and opening secure containers, said secure	2^{nd} consumer's computer receives Windows Media file (secure container) via	second Printshop CUPID Client	same as (a)(5) for 2^{nd} apparatus	2^{nd} apparatus and/or associated	"Secure container" is transmission

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	running on the second Unix Server is responsible for receiving a) content files from another CUPID Client, and b) messages from the Origination Server Message Queue		processes.	(datastream or file) sent from sender computer to recipient computer. The transmission includes a message (the "governed item") sent by Alice to Bob, which is encrypted with the (shared secret) session key K_{AB}. Network adapter, networking protocol software, Kerberos protocol software or hardware, and decryption software (e.g., DES decryptor) are used to receive and open Alice's message on the recipient computer.
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules in combination	see 28(a)(6)	same as (a)(6) for 2nd apparatus	SOODB process and/or object methods in the trusted computing base. "Secure container rule" is received from third system where the class for the remote object is persisted. Rule implements some control over access to object, such as multi-level security or method authorization	"Secure container rule" is any of the other three of the four values in the recipient ticket. Note that the sender and recipient IDs in the recipient ticket actually originates from the initial ticket request from the sender computer to the KDC server. All four values in the recipient ticket are applied in combination to govern use of the session key to access (decrypt) Bob's message. "PPE" is the Kerberos protocol software on the recipient computer.
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 28(a)(7)	same as (a)(7) for 2nd apparatus	Any hardware or software allowing interconnection and intercommunication in the distributed SOODB	Sender computer's network card and networking protocol software.
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	any Agent application running on said second Unix Server responsible for clearing rights, or authorizing rights, for use of content in subdocument files, such as art, images or research materials	any "intermediary" account, such as an administrative account or root, or credential server	Electronic "intermediary" is a downgrading process or other system process specifying and resolving multi-level security concurrency conflicts or resolving covert channel problems	The Kerberos key distribution center (KDC).
29. A system as in claim 28,					
said user rights authority clearinghouse	License Issuer, operatively connected to	28(c) above, "operatively	28(c) above, "operatively	system of 28(c), e.g., Downgrader	KDC is networked with sender's,

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
operatively connected to make rights available to users.	consumer's computer (WMRM SDK, Step 9)	connected" to user(s)	connected" to users	process is "operatively connected" to the SOODB as is the resolver process.	recipient's and others' computers to provide the tickets.

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust) (continued)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
2. A system including:		Reference is made to Cox, Brad J., "SUPER DISTRIBUTION AND ELECTRONIC OBJECTS - What if there is a silver bullet...and the competition gets it first?" (Dr. Dobbs Journal, Oct. 1992)), discussing e.g. Mori, Ryoichi and Masaji Kawahara, "Superdistribution: The Concept and the Architecture," Transactions of the IEICE, vol. E 73 (July, 1990). (A version of this Cox article first appeared in the Journal of Object-oriented Programming (June, 1992); see also Cox, Brad J. "There is a Silver Bullet." BYTE (October, 1990)).	Reference is made to Gary Griswold, "A Method for Protecting Copyright on Networks," in IMA/CNI 94, above, and the demo version referenced therein; see also WO93/01550	Reference is made to IBM Corp.'s "Cryptolope" system and software (hereafter "C") Reference is made to "iOpener System Description," (National Semiconductor 1993) ("iO"), and National Semiconductor's "iPower" product(s), including as publicly proposed or disclosed in combination with EPR & "VDE" ("iP")	Reference is made to Lampson, et al., Authentication in Distributed Systems, ACM 1992. See also, e.g., Authentication and Delegation with Smart Cards, M. Abadi, M. Burrows, C. Kaufman, and B. Lampson *Science of Computer Programming* 21, 2 (Oct. 1993), pp 91-113; Authentication in the Taos Operating System (1993).
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	vendor or clearinghouse or consumer device having an S-box, e.g. an S-computer	user's computer	user's computer	any computer in the distributed network
(1) user controls,	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	has user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	a comm-port
(3) a processor,	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	a processor
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	and a memory
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been	Secure container (packaged Windows Media file), received by consumer's computer from	e.g. S-software, S-programs, music, &/or payment files	software envelope	C: Cryptolope iO, iP: at least partly	fields of credential received from 2d apparatus may be encrypted, e.g. identity of principle making the

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
received from a second apparatus;	"Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")			encrypted data received by user	request embodied in the "governed data item"
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	vendor et al. can supply one or more "rules" and can cancel privileges; "rules" can also be in account file information, or credit limits set or reset by sales outlets or agents. Files are also subject to access rules, authentication of user by host, etc.	central authorizing site governs aspects of use and/or access	C: "rights portion" of e.g. "license cryptolope" iO: UMS can supply "rules" (or content)	the verification information received from appliance 3 is a "rule" according to InterTrust
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	software and/or hardware for receiving and opening S-software	see 2, above	see 2, above	"first apparatus" could be hardware and software for "secure" processing; "governed item" is e.g. request by principle at "second apparatus"
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	tamper-resistant environment, and S-boxes or S-software	see 2, above	see 2, above	first apparatus is a "protected processing environment" according to InterTrust; "rules" is vague but as used alleged by InterTrust in this litigation would include access controls and capabilities, and data integrity
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	a public or private network	a network	a network	nodes transmit and receive
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(3) a processor,	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right	see 2, above	see 2, above	see 2, above	See 2(a)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
	received as part of a signed license (WMRM SDK, Step9)				
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	see 2, above	see 2, above	see 2, above	See 2(a)(5)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	see 2, above	see 2, above	see 2, above	See 2(a)(6)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 2, above	see 2, above	see 2, above	See 2(a)(7)
(b) a second apparatus including:	2nd consumer's computer	see 2, above	see 2, above	see 2, above	any 2d node
(1) user controls,	2nd consumer's computer	see 2, above	see 2, above	see 2, above	See 28(b)
(2) a communications port,	2nd consumer's computer	see 2, above	see 2, above	see 2, above	See 28(b)
(3) a processor,	2nd consumer's computer	see 2, above	see 2, above	see 2, above	See 28(b)
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	see 2, above	see 2, above	see 2, above	See 2(a)(4)
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	see 2, above	see 2, above	see 2, above	See 2(a)(5) e.g. the verification info is a "rule" according to InterTrust; it verifies the certificate and decrypts the encrypted portion
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules	see 2, above	see 2, above	see 2, above	See 2(a)(6)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
to at least in part govern at least one aspect of access to or use of a governed item;	in combination				
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 2, above	see 2, above	see 2, above	See 2(a)(7)
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	a "clearinghouse" or permissions and/or rights "issuer"	license server	C: royalty/ license clearing center, or smart card iO: UMS iP: e.g. "VDE"	certificate authority
29. A system as in claim 28,					
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	see 28(c)	System of 28(c)	System of 28(c)	System of 28(c)

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
2. A system including:		Reference is made to S. Muftic, <u>Security Mechanisms for Computer Networks</u> (Halstead Press, a div. of John Wiley & Sons, 1984)	See deciphering techniques, methods, systems and procedures described in e.g. Kahn, Denning, Muftic, Davies, PEM, and <u>Computer Security</u> (Time Life 1990).	eference is made to the Hellman references cited in the asserted patents, including USP 4,658,093, "New Directions," and "Multi-user Cryptographic Techniques."	Reference is made to D. Denning, "Secure Personal Computing in an Insecure Network," Comm. of the ACM, vol. 22 No. 8 (August 1979); See also, e.g., D. Denning, <u>Cryptography and Data Security</u> (Addison-Wesley 1982)
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	Any computing device, e.g. a computer associated with receiver B (e.g., a merchant) receiving a cheque.	The above references plainly indicate that a networked and/or stand-alone computer may be used to perform the steps of such techniques, methods and procedures.	player and/or base unit	any user's computer (see, e.g., Figs. 2-5)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	has user controls	see 2(a)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a comm port	see 2(a)
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a processor	see 2(a)
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	and a memory	see 2(a)
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	Secure container (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")	Encrypted cheque transmitted by A and stored in a memory location associated with B containing signature, value, date etc.	an at least partly encrypted message or file (e.g., signed and/or sealed using a symmetric or asymmetric method)	program from 2d apparatus (e.g. purchased at store or by phone) that requires authorization to be used	a file F, message X, or "secure" communication, containing any encrypted content
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	"rules" (such as validity time, check number, ID etc.) used to "open" and validate the cheque, and/or Secret Key (SKC) provided by the bank C	the deciphering code, tool. algorithm and/or data	any of one or more rights or requirements received from a 3d apparatus, such as signed authenticator and/or base unit or key info	file access rules and/or authorization and/or authentication and/or keys obtained from another apparatus, e.g.detachable S-key device, Alt-P generating software, another computer, or Central Facility
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	system hardware or software used for e.g. "receiving" and "opening" electronic cheques	deciphering system hardware or software	system hardware or software	software or hardware for receiving and opening files, messages, and/or communications
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	receiver B system uses keys provided by A and C and/or specified value, date, validity time, check no., ID etc. to "open" and validate electronic cheques	any 2nd "rules" used in deciphering the message, such as in the algorithm, data or method used to verify a signature or decrypt or display a file or message	processing has safeguards; see above re e.g. BLP "rules," which Hellman supplements (see '193 chart)	systems can be confined, and/or keys recorded in sealed memory chip or magnetic stripe card
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	Any hardware or software used to receive or transmit electronic cheques	system hardware or software used to receive or transmit files or messages	hardware or software is used for transmission	a public or private network
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right received as part of a signed license (WMRM SDK, Step9)	See 2(a)(4) above	See 2(a)(4)	See 2(a)	see 2, above
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 2(a)(5)	See 2(a)(5)	See 2(a)	see 2, above
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	Hardware or software that uses "rules" such as ID, date, value limits, check no., validity time to access, open and sign cheques; see also 2(a)(6)	See 2(a)(6)	See 2(a)(6)	see 2, above
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	Hardware or software used to transmit checks, keys etc. between entities A, B and/or C	See 2(a)(7)	See 2(a)(7)	see 2, above
(b) a second apparatus including:	2nd consumer's computer	Any computer associated with a 2nd receiver B (e.g., a 2nd merchant)	a 2nd computer used for deciphering messages or files	any second user's computer	see 2, above
(1) user controls,	2nd consumer's computer	See 28(b) above	See 28(b)	See 28(b)	see 2, above
(2) a communications port,	2nd consumer's computer	See 28(b) above	See 28(b)	See 28(b)	see 2, above
(3) a processor,	2nd consumer's computer	See 28(b) above	See 28(b)	See 28(b)	see 2, above
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	See 28(a)(4); 2nd "rule" may be ID, date, or signature of A that is unique to a given cheque	See 28(a)(4)	See 2(a)(4)	see 2, above
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via	See 28(a)(5)	See 28(a)(5)	See 2(a)(5)	see 2, above

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
with each of said secure containers;	Windows Media Player and Windows Media Rights Manager.				
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules in combination	See 28(a)(6)	See 28(a)(6)	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	see 2, above
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	Hardware or software used to transmit cheques between entities	system hardware or software for transmitting files or messages	See 2(a)(7)	see 2, above
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	Bank C	any "intermediary" computer with a "clearinghouse" function	authorization and billing unit	a Central Facility
29. A system as in claim 28,					
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	Bank C "operatively connected" to plural merchants	"operatively connected" to more than one computer used to decipher messages	system of 28(c)	see 28(c)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

U.S. PATENT NO. 6,253,193 (invalid as alleged by InterTrust)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
1. A method comprising:								
(a) receiving a digital file including music;	Reference is made to the Windows Media Rights Manager SDK Programming Reference ("WMRM SKD"), attached hereto as Exhibit A. Media Player infringement analysis is set forth herein using the example of a music file downloaded and transferred to a portable audio player. Consumer receives a Windows Media file (WMRM SDK, Step 3)	See references in '683 chart above, e.g., USP 5,634,012; 5,715,403; 5,629,980; and 5,638,443; col:line references below refer to the '012 patent. One kind of digital work received at a first device can be an audio file. See e.g., 8:26 ("Examples of a rendering system may be a computer system, a digital audio system, or a printer") 16:8 (Examples of high value works include movies, digital music) 20:41 (Grammar element "1504 Render-Code" takes values for "Play" for playing, e.g. "digital movies, digital music, playing a video game, running a computer system") 37:51-66 (typically to "play" a work is to use a transducer, e.g. speaker or display) 50:15 (example of pay-per-use application: music demo) "A musician may want to allow extraction of portions of his work but not changing of the tonality"	See reference cited in '683 chart above. "Document" includes audio clips or movies (p1), e.g., MIDI or QuickTime	See Blaze references listed above. Receiving any music file (e.g. MIDI or music program) transferred from one computer or medium to another. As noted in the accompanying text, and as expressly indicated in e.g. Stefik, Choudhury, Hellman, etc., it was obvious that protections might be applied to digital music.	See references in '683 chart above. In e.g. Linn, user (e.g., library or distributor) receives an audio file	See references in '683 chart above, (e.g. US Patent No. 4,658,093) . E.g. a customer or store (or other distributor, manufacturer or vendor) receives file including music	See references cited in '683 chart above. Publisher's CUPID Client transmits files and job ticket information to the Origination Server. As noted in the accompanying text, and as expressly indicated in e.g. Stefik, Choudhury, Hellman, etc., it was obvious that protections might be applied to digital music.	Reference is made to the Neuman and Chaum references cited above (see '683 chart). As noted in the accompanying text, and as expressly indicated in e.g. Stefik, Choudhury, Hellman, etc., it was obvious that protections might be applied to digital music.

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
		52:53-58 (definition of Digital Work is "encapsulated digital information such as music")						
(b) storing said digital file in a first secure memory of a first device;	Windows Media file is stored in consumer's computer and all use of it is securely managed by the Secure Content Manager in Windows Media Player.	Digital works are stored in secure repositories, e.g. repository 201 in Fig. 1 8:27 ("A rendering system has the same security features as a repository") 16:7-15 (repositories suitable for holding valuable digital works like bearer bonds & first run movies can have "elaborate measures for ensuring physical integrity and for verifying authorization before use") See col. 16, Table 2 (Repository security levels 0-10)	client or server memory	file stored in a device	object is stored in a form which may not be displayed or printed without the rendering software unless it is extracted from within its envelope and is an authorized copy	stores files "securely," using one or more techniques or combination thereof (e.g., permissions, ACLS, logins, keys and locks, physical security)	Origination Server packages the file content into a Printjob	exchange of music file (e.g. data or audio programming or multimedia) using budgets and other authorization and authentication techniques and capabilities of Neuman and/or Chaum.
(c) storing information associated with said digital file in a secure database stored on said first device, said information including at least one budget control and at least one copy control, said at least one budget control including a budget specifying the number of copies which can be made of said digital file; and	License is stored in the License Store (WMRM SDK, Step 5); license includes Rights which may include AllowTransferToNonSDMI, AllowTransferToSDM.	- info associated with music file can include usage rights, expressed in a URG (usage rights grammar). See list at Fig. 15: Control examples include: Right Code (e.g. Transport code, including right to copy, transfer, loan), Derivative Work Code, & Next-Set of Rights; Budget control examples include Copy Count. See also Fig. 10 (rights portion of designation block of Fig. 7): includes rights code 1050 and status info 1052 7:61 (authorization/digital certificate can itself be a digital work that moves between repositories subject to usage rights)	"documents" may have different levels of security, rendering requirements, granular levels of billing and access, access control, authentication (including Kerberos), persona, anonymous. See '683 ¶ 2(a)(4)(ii)	operation budget and copying information associated with file is stored (e.g., by or for root or other user of certain level or privilege) on device	active and passive protections control copying; authorized use meter and/or "copy counter" can be employed to limit number of copies	Stores associated budget control and/or copy information in secure manner	Scenario A) the Workflow Management Service stores data e.g. for tracking dates and file removal Scenario B) Each Printjob created contains a specified header including copy counters. The budget control is in the header of each Printjob record that is created.	storing associated at least one "budget" and "copy control" for commerce and/or other management or policy

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
said at least one copy control controlling the copies made of said digital file;								
(d) determining whether said digital file may be copied and stored on a second device based on at least said copy control;	Windows Media Rights Manager enforces the license restrictions	Usage right(s) (e.g. Transport-Code, Time-Spec determine whether the file can be copied, e.g. to rendering repository 203 in Fig. 2. Repository 201 is coupled to a rendering device to comprise a "rendering system" 7:66-8:3, 8:22 et seq.)	e.g., rights/permissions/ credentials determine whether the file can be copied to 2d device	directory and/or file keys, permissions, rights, and/or privileges determine whether file may be copied to 2nd device	-"write protect" status determines whether can copy - rendering program determines whether to copy and store on an output device, e.g. a video display or printer or audio device	determines whether file may be copied to base unit or player, or played (e.g. to be recorded on another device while playing)	Origination Server governs whether files can be transferred; CUPID clients receive files based on information they receive via their message queues and notification servers	One or more rights, permissions, keys and/or credentials effect "copy control"
(e) if said copy control allows at least a portion of said digital file to be copied and stored on a second device,	Windows Media Rights Manager determines whether the AllowTransferToNonSDMI or AllowTransferToSDMI rights are present	if copy is allowed,	if copy is allowed,	if allowed to copy	if allowed	if allowed,	if allowed	if allowed,
(1) copying at least a portion of said digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	a copy is made,	a copy is made,	a copy is made	a copy is made	copy is made,	a copy is made	copy is made,
(2) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;	Portable device necessarily includes at least a memory and audio output.	and transferred to the memory of the rendering repository; the music file is stored in a repository, either ephemerally or permanently (or it could be stored in the music-equivalent of the "printer repository" of 8:39-46)	and transferred to a memory of 2d device with a speaker and/or video output	file is copied to a 2nd device including a memory and an audio and/or video input (e.g. a PC)	2d device includes a memory and audio and/or video output	and transferred to a 2d device which includes a memory and audio and/or video output	and transferred to a 2d device which includes a memory and audio and/or video output	and transferred to a 2d device which includes a memory and audio and/or video output
(3) storing said digital file in said memory of said second device; and	Music file is transferred to the portable device	file is transferred	file is transferred	storing the file in the 2nd device's memory	"document" is transferred	where it is stored	CUPID Client stores	where it is stored
(4) including playing said	Portable device plays the music	Played, in URG sense and in sense of being rendered (e.g. 20:41)	and played	music played	render on 2d device	and played	and renders	and played

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
music through said audio output.								
2. A method as in claim 1, further comprising:								
(a) at a time substantially contemporaneous with said transferring step, recording in said first device information indicating that said transfer has occurred.	Counter reflecting TransferCount is decremented by Windows Media Rights Manager	e.g. Copy Count or remaining loan is a variable	transfer information recorded	system/host logs transfer event and e.g. CPU time and/or memory	library/distributor records transfer to 2d device (e.g., library may record "loan")	accounting for transfer	Origination Server decrements count for Printjob	transfer accounted for
3. A method as in claim 2, in which:								
(a) said information indicating that said transfer has occurred includes an encumbrance on said budget.	Counter decrement reduces the allowable number of budgeted transfers	Total Copy Count, or total loan ability, are "budget" values that get decremented. See also Table 1 (Digital Work State Information).	encumbering a "budget"	transfer encumbers a "budget"	permitted number of copies decremented	transfer reduces number of allowable transfers	see 2(a)	by an "encumbrance" on the "budget"
4. A method as in claim 3, in which:								
(a) said encumbrance operates to reduce the number of copies of said digital file authorized by said budget.	Counter decrement reduces the allowable number of budgeted transfers	Copying or loaning reduces the number of authorized copies	reducing the number of authorized copies	encumbrance operates to reduce remaining number of copies authorized by user budget	see 3(a)	transfer reduces number of allowable transfers	see 2(a)	transfer can reduce number to be allowed
11. A method comprising:								
(a) receiving a digital file;	onsumer receives a Windows Media file (WMRM SDK, Step 3)	See 1(a)	See 1(a)	Host receives encrypted file	File is a "sealed object"	See 1(a)	See 1(a)	See 1(a)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
(b) storing said digital file in a first secure memory of a first device;	Windows Media file is stored in consumer's computer and all use of it is securely managed by the Secure Content Manager in Windows Media Player.	See 1(b)	See 1(b)	Stores in memory managed by Unix/CFS	storing file in memory of a device	See 1(b)	See 1(b)	See 1(b)
(c) storing information associated with said digital file in a secure database stored on said first device, said information including a first control;	License information is stored in the License Store (WMRM SDK, Step 10), license information includes Rights. License Rights may include AllowTransferToNonSDMI, AllowTransferToSDMI, LicenseCount	See 1(c) E.g., "Certain communications and transactions may be conditioned on a repository being in a particular security class."	rights and levels stored in memory	Information associated with the file is stored in memory (e.g., a CFS directory) by Unix/CFS and includes a first "control" (e.g., a particular permission or right or key)	storing "control" information in memory	usage rights or access controls	Origination Server creates Printjob, uses Workflow Management Service, records requirements, tasks and prerequisites needed in order to process	storing any of numerous positive or negative credentials, rights, or restrictions associated with file
(d) determining whether said digital file may be copied and stored on a second device based on said first control,	WMRM determines whether transfer rights are included in license (WMRM SDK, Step 5)	No copy is stored on 2d repository (or the rendering hardware) if the usage rights and/or security level information and/or access controls don't allow it	copy made or not depending on a "control"	Based on the "control," determines whether file can be copied to 2nd device	control may be used to determine whether file can be copied to 2d device using the rendering software	copy made or not depending on a "control"	Origination Server checks copy controls to determine whether to transfer Printjob to Printshop	copy made or not depending on a "control"
(1) said determining step including identifying said second device and determining whether said first control allows transfer of said copied file to said second device, said determination based at least in part on the features present at the device to which said	Portable Device Service Provider Module identifies the portable device as either SDMI-compliant or non-SDMI-compliant and provides this information to Windows Media Device Manager, which allows the transfer based on whether the device identification matches the License Right.	Usage rights, security level check and/or access control check may fail based on 2d device's identity	checking 2d device	2d device may be identified and transferability determined based on one or more of its features	based at least in part on features of 2d device (e.g., does user have "write" privileges to 2d device; or is the user identification a match; or is the 2d device able to receive data, e.g. using a given protocol)	2d device may be identified and transferability determined based on one or more of its features	Origination Server initiates contact with Notification Server running at Printshop and requests the PSP (Printshop Specification Record) containing information regarding the capabilities of the Printshop	2d device may be identified and transferability determined based on one or more of its features

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Steflk	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
copied file is to be transferred;								
(e) if said first control allows at least a portion of said digital file to be copied and stored on a second device;	If Windows Media Rights Manager determines whether the AllowTransferToNonSDMI or AllowTransferToSDMI rights are present, the following steps are performed:	depending on the usage rights/security level/ACL check	depending on the check results	If the control allows the copying	if copy is allowed	if copy is allowed	If the PSP specifications match those required by the Printjob,	if copy is allowed
(1) copying at least a portion of said digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	a copy may be made	copy may be made	The file is copied	copy may be made	copy may be made	CUPID Client is notified that the Printjob is available to be received	copy may be made
(2) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;	Portable device necessarily includes at least a memory and audio output	and transferred to a 2d repository with video and/or audio output	and transferred to 2d device with video and/or audio output	To a device with video and/or audio output (e.g., a PC)	and transferred to 2d device with video and/or audio output	and transferred to 2d device with video and/or audio output	file transferred	and transferred to 2d device
(3) storing said digital file in said memory of said second device; and	Music file is stored in the portable device	stored there	stored there	Stored in memory	stored there	stored there	stored	stored there
(4) rendering said digital file through said output.	Portable device plays the music	and rendered through audio and/or video output	and rendered	And rendered	and rendered	and rendered	and rendered	and rendered
15. A method comprising:								
(a) receiving a digital file;	onsumer receives a Windows Media file (WMRM SDK, Step 3)	A digital work is received	User receives a file	An encrypted file is received at e,g, host or user divice	File received	Vendor or base unit receives file	Origination Server receives digital file from CUPID Publisher Client	File received
(b) an authentication step comprising:							Publisher logs in to authenticate identity	
(1) accessing at	License includes identity of	See Table 2. Various authentication	user or "device"	"device" or user	user or "device"	check for base unit;	Publisher assigns an	user or "device"

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
least one identifier associated with a first device or with a user of said first device; and	user's Windows Media Player	"identifiers" can be accessed. "A repository will have associated with it a repository identifier. Typically, the repository identifier would be a unique number assigned to the repository at the time of manufacture. ... As a prerequisite to operation, a repository will require possession of an identification certificate. Identification certificates are encrypted to prevent forgery and are issued by a Master repository." - Works can be signed - Passwords can be associated with users or devices - Physical security comprises known authentication steps	"identifier" accessed according to InterTrust	"identifier" accessed, e.g., login or password or signature or address or number	"identifier" accessed according to InterTrust	or check e.g. password or ACL or key	Order Name and authorization codes for documents	"identifier" accessed according to InterTrust
(2) determining whether said identifier is associated with a device and/or user authorized to store said digital file;	Music file cannot be used unless identifier indicated in License matches user's Windows Media Player identifier	authentication succeeds or fails	authentication succeeds or fails	authentication succeeds or fails	authentication succeeds or fails	authentication succeeds or fails	Checks login, or authorization codes against valid system users via standard Unix login measures or through secure PKI authentication techniques	authentication succeeds or fails
(c) storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized.	Music file will not be processed through Windows Media Player, including protected rendering buffers, unless the identifiers match	Digital work is stored in repository only if authentication succeeds	file is "processed" only if authentication succeeds	"storing" occurs if authorized	file is "processed" only if authentication succeeds	file is "processed" only if authentication succeeds	If authorized as a valid document publisher, the Origination Server allows the files to be stored on the Origination Server; see 1(a)	file is "processed" only if authentication succeeds
(d) storing	License includes Rights and is	associated usage right(s) or security	license rights	see 11(c)	attributes are stored	rights include limits	See 11(c)	See 11(c)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
information associated with said digital file in a secure database stored on said first device, said information including at least one control;	stored in the License Store, Rights may include AllowTransferToNonSDMI, AllowTransferToSDMI, LicenseCount	level information is stored on 1st device; see also 11(c)	include limits on transfer; see also 11(c)		with associated object; see also 11(c)	on transfer; see also 11(c)		
(e) determining whether said digital file may be copied and stored on a second device based on said at least one control;	Windows Media Rights Manager enforces the license restrictions	System enforces usage rights and levels	See 11(d)	See 11(d)	rendering software enforces restrictions	See 11(d)	See 11(d)	See 11(d)
(f) if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	If appropriate rights are present, the following steps are performed:	if copying and storing a portion of file is allowed	See 11(e)	See 11(e)	if copying and storing a portion of file is allowed	See 11(e)	See 11(e)	See 11(e)
(1) copying at least a portion of said digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	The digital work is copied	See 11(e)(1)	copies if permitted	at least a portion is copied	file or portion copied	See 11(e)(1)	See 11(e)(1)
(2) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;	Portable device necessarily includes at least a memory and audio output	and transferred to 2d repository	See 11(e)(2)	2nd device includes memory and audio and/or video output (e.g., PC has monitor and/or speaker)	and transferred to 2d device	and transferred	See 11(e)(2)	See 11(e)(2)
(3) storing said digital file in said memory of said second device; and	Music file is stored in the portable device	where it's stored	See 11(e)(3)	file is stored	stored there	stored	See 11(e)(3)	See 11(e)(3)
(4) rendering said digital file	Portable device plays the music	and rendered	See 11(e)(4)	and rendered	and rendered	and rendered (e.g., at base unit, or at	See 11(e)(4)	See 11(e)(4)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Steflk	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
through said output.						player or other 2d device)		
19. A method comprising:								
(a) receiving a digital file at a first device;	WMRM SDK, Step 3.	A digital work is received at a first repository	file received	Receive file at device (e.g., download or floppy at "device" on Unix/CFS network, e.g. earlier in or in earlier session).	user receives file	file received	Origination Server	file received
(b) establishing communication between said first device and a clearinghouse located at a location remote from said first device;	WMRM SDK, Step 6.	any 2nd repository, including but not limited to a billing repository, can act as a "clearinghouse" communicating w/ a physically remote 1st repository	communication established with repository acting as "clearinghouse" (see '683 ¶ 28(c))	establish communication with any "clearinghouse" device in Unix/CFS network	user communicates with any "clearinghouse" device, e.g. library	communication with any "clearinghouse" device, e.g. vendor or authorization unit	Agent running at the Origination Server communicates with a "clearinghouse"	"clearinghouse" as alleged by InterTrust is met by any certificate server or other device capable of transacting with multiple users
(c) said first device obtaining authorization information including a key from said clearinghouse;	WMRM SDK, Step 9.	"clearinghouse" repository provides authorization information "including a key"	"clearinghouse" supplies authorization information "including a key"	Device obtains key from system	user obtains authorization info	"clearinghouse" supplies authorization information "including a key"	Agent running at Origination Server checks to see if included subdocument files are authorized for use by the publisher, and receives authorization notification from clearinghouse	"clearinghouse" supplies authorization information "including a key"
(d) said first device using said authorization information to gain access to or make at least one use of said first digital file, including using said key to decrypt at least a portion	WMRM SDK, Step 11.	Authorization information used for access or use (& key use to decrypt digital work, which may be usage rights)	authorization information used for access or use	Device uses key to decrypt at least a portion of the file	authorization information used for access (e.g., uses file's public key to decrypt its signature)	authorization info used for access or use	E.g. stock image files may be partly encrypted; access to images must be granted through clearinghouse servers and payment servers, allowing subdocuments to be transmitted to the	key used to decrypt

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
of said first digital file; and							Origination Server, decrypted and ultimately included into final Printjob by Document Assembly Service	
(e) receiving a first control from said clearinghouse at said first device;	WMRM SDK, Steps 8-9.	one or more "controls" is received from "clearinghouse" repository	one or more "controls" received from "clearinghouse"	Receives file permissions or key	a "control" comes with the file	a first "control" received	Right to reproduce authorization is received by Origination Server	a first "control" received
(f) storing said first digital file in a memory of said first device;	WMRM SDK, Step 3.	Digital work stored in a 1st device's memory	File stored	File stored	File stored	File stored	File stored, E.g. Workflow Management Service communicates with Document Assembly Service that creates printable materials by assembling subdocuments referenced during publishing step	File stored
(g) using said first control to determine whether said first digital file may be copied and stored on a second device;	At least the following WMRMRights Object properties meet this limitation: AllowTransferToNonSDMI, AllowTransferToSDMI TransferCount	"control" determines whether file can be copied to 2d device	"control" determines whether file can be copied to 2d device	Uses permissions or key to determine whether can copy to another device	"control" determines whether file can be copied to 2d device	and used to determine whether file maybe copied and stored on 2d device	Authorization is checked prior to including files in Printjob	and used to determine whether file maybe copied and stored on 2d device
(h) if said first control allows at least a portion of said first digital file to be copied and stored on a second device;	This and all subsequent claim steps occur when the condition specified in the WMRMRights Object property is met	if the copying is allowed	if the copying is allowed	If permission key allows or signature works	if the copying is allowed	if copy is allowed	If Authorization is granted then the file can be copied	if copy is allowed
(i) copying at least a portion of said first digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	copying occurs	copy made	The file is copied	copy made	a copy may be made	CUPID Client copies	a copy maybe made
(j) transferring at	Portable device necessarily	the work is transferred	transferred	Transferred to a 2nd	transferred	transferred	transfers	transferred

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
least a portion of said first digital file to a second device including a memory and an audio and/or video output;	includes at least a memory and audio output			device with memory and audio and/or video output				
(k) storing said first digital file portion in said memory of said second device; and	Music file is stored in the portable device	stored in the 2d device	stored	Stored in 2nd device memory	stored	stored	stores	stored
(l) rendering said first digital file portion through said output.	Portable device plays the music	and rendered through audio and/or video output	and rendered	And rendered.	and rendered	and rendered	and renders	and rendered

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

DERWIN & SIEGEL, LLP
DOUGLAS K. DERWIN - #111407
3280 Alpine Road
Portola Valley, CA 94028
Telephone: (408) 855-8700
Facsimile: (408) 529-8799

INTERTRUST TECHNOLOGIES CORPORATION
MARK SCADINA - #173103
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA
AND COUNTER ACTION.	**INTERTRUST'S OPENING CLAIM CONSTRUCTION BRIEF** Date: May 12, 29, & 30, 2003 Time: 9:00 a.m.

TABLE OF CONTENTS

TABLE OF CONTENTS
(cont'd)

TABLE OF CONTENTS
(cont'd)

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

TABLE OF AUTHORITIES
(cont'd)

I. INTRODUCTION

This case pits a small, innovative industry pioneer against a monopolistic giant whose ruthless, anticompetitive tactics are legendary. InterTrust invented the field of Digital Rights Management ("DRM"). Microsoft praised InterTrust's work as revolutionary, negotiated with InterTrust for a license to InterTrust's technology and patents, then broke off negotiations and unilaterally designed InterTrust's innovations into a large portion of Microsoft's product line.

InterTrust, however, has one asset Microsoft's other victims did not possess: long before Microsoft had even heard of Digital Rights Management, InterTrust filed foundational patents in the field, patents that now read directly on major Microsoft initiatives in this area.

Microsoft now seeks to avoid the consequences of its actions by urging this Court to adopt claim constructions that would render the InterTrust claims meaningless. Microsoft would have this Court read a single, two thousand word definition into every single InterTrust claim, a definition at least twenty times longer than any claim construction ever adopted by any Court, and almost certainly far longer than any definition ever even proposed. No jury could possibly comprehend Microsoft's two thousand word definition, much less apply it in any meaningful way.

Nor could any jury meaningfully apply numerous other claim construction proposals from Microsoft, many of which amount to hundreds of words of highly complicated text. Microsoft's constructions improperly read dozens of detailed limitations from specification embodiments into the claims and incorporate numerous other restrictions that contradict the specifications or are made up from whole cloth. Microsoft's proposed definitions are inconsistent with fundamental canons of claim construction.

By contrast, InterTrust's straightforward claim constructions conform to the plain language of the claims, informed by the specifications, and provide a clear and informative blueprint that can easily be understood and applied by the trier of fact. That a straightforward approach compels a finding of infringement may not be to Microsoft's liking, but it is what the law requires.

II. FACTUAL BACKGROUND

The InterTrust patents involved in this litigation derive from a foundational patent application filed in February 1995. That application resulted from a number of years of concentrated work by the four inventors, starting with an investigation first begun by InterTrust founder Victor Shear in the 1980s.[1] From InterTrust's inception in 1990 and throughout the following decade, Mr. Shear and his colleagues tackled the most intractable difficulties confronting the digital marketplace: how to enable authors, publishers, and other owners of digital content to distribute and sell that content electronically, while simultaneously protecting that content from misuse and piracy. InterTrust not only saw the problems that currently plague electronic commerce, it discovered crucial solutions, and then described those solutions in the patents that are the subject of this claim construction brief.

The foundational InterTrust patent application describes an overall "architecture" for Digital Rights Management, an integrated approach designed for conducting trusted and secure electronic commerce.[2] InterTrust's inventors began thinking about these concepts long before the rest of the computer industry, and literally years before Microsoft had given any thought whatsoever to DRM.

InterTrust's design and approach were widely recognized in the industry as groundbreaking and revolutionary. For example, one senior Microsoft executive was quoted as follows:

> "InterTrust is solving problems that won't be in the mainstream for quite some time," says Will Poole, senior director of marketing and business development at Microsoft's Streaming Media Division. "It's visionary."

The Wall Street Journal, April 29, 1999, Page Decl. Exh. A. The InterTrust patents were also recognized in the industry as fundamental: "'Before anybody had thought about this stuff, [Victor Shear] was out there patenting it,' said Kirk Loevner, a former Apple Computer Inc.

[1] See Declaration of Michael Page ("Page Decl."), Exh. A, for a more detailed history of InterTrust. See also Shear Deposition Transcript 157:13-158:23 (Page Decl., Exh U); Supplemental Response of Plaintiff InterTrust Technologies Corp. to Defendant Microsoft Corporation's First Set of Interrogatories (Page Decl., Exh. V).

[2] See Declaration of Dr. Michael Reiter ("Reiter Decl."), ¶¶ 10-15.

executive." Id.

Starting in 1998, Microsoft negotiated for a license to InterTrust's technology and patents. These negotiations involved literally dozens of meetings, at which InterTrust made significant disclosure of its technical architecture. In 2000, Microsoft terminated these discussions. In the same timeframe, Microsoft announced its .NET initiative, a major Microsoft project designed to incorporate DRM into all aspects of Microsoft's products. This lawsuit followed.

III. CLAIM CONSTRUCTION PRINCIPLES IN GENERAL

The landmark case of Markman v. Westview Instruments, Inc., 517 U.S. 370 (1996), made claim construction a question of law for this Court to decide. Since Markman, the Federal Circuit has progressively refined the claim-construction process and established a detailed methodology for construing patent claims.

In its significant recent opinion in Texas Digital Systems, Inc. v. Telegenix, Inc., 308 F.3d 1193 (Fed. Cir. 2002), the Federal Circuit synthesized the claim construction process and, in doing so, defined a roadmap for construing patent claims. First, the ordinary meaning of each disputed term is determined. Id. at 1202, 1204. There is a "heavy presumption" that claim terms should be interpreted to "have the ordinary meaning that would be attributed to those words by persons skilled in the relevant art." Id. at 1202. The Federal Circuit encourages examination of "relevant dictionaries, encyclopedias and treatises" to determine how those in the art would understand the claim. Id. at 1205.

The Federal Circuit has warned against considering the specification and file history during this initial step:

> Consulting the written description and prosecution history as a threshold step in the claim construction process, before any effort is made to discern the ordinary and customary meanings attributed to the words themselves, invites a violation of our precedent counseling against importing limitations into the claims.

Id. at 1204. To avoid this error, the court must first focus on the claim's ordinary meaning.

Second, the patent's specification and prosecution history are examined for clear evidence tending to rebut the presumption that a term should be given its ordinary meaning. Id.

at 1204 ("In short, the presumption in favor of a dictionary definition will be overcome where the patentee, acting as his or her own lexicographer, has clearly set forth an explicit definition of the term different from its ordinary meaning."). Such evidence may include use of the term in the specification "in a manner clearly inconsistent with [its] ordinary meaning" and "expressions of manifest exclusion or restriction" by an inventor that clearly disavow or disclaim scope that would have otherwise been encompassed by the term. Id.

"[U]nless compelled otherwise, a court will give a claim term the full range of its ordinary meaning as understood by persons skilled in the relevant art." Id. at 1202. Thus, a term's ordinary meaning must be adopted unless clear evidence from the patent's specification or prosecution history manifests a departure from the standard usage of the term. Id.

The claim's central role in defining a patentee's invention is also the basis for one of the most well-established canons of claim construction: the prohibition against reading features or limitations into a claim from the patent specification. See, e.g., McCarty v. Lehigh Valley R.R., 160 U.S. 110, 116 (1895) ("[W]e know of no principle of law which would authorize us to read into a claim an element which is not present"); Renishaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1248 (Fed. Cir. 1998). This rule follows from the separate purposes of the patent specification and claims. The role of the patent specification is to adequately describe the invention to enable the public to make and use it once the patent expires. See 35 U.S.C. § 112, ¶ 1. The role of the claims is completely different. See SRI Int'l v. Matsushita Electric Corp. of Am., 775 F.2d 1107, 1121 n.14 (Fed. Cir. 1985) ("Specifications teach. Claims claim.").

Patent claims define the inventor's property right. A patent claim recites a particular combination of elements that the inventor believes is different than any combination that has existed before. If it is novel, and is also useful and not obvious, the inventor is entitled to a patent monopoly for the claimed combination even if it does not include many elements of the inventor's preferred embodiment described in the specification. See, e.g., Renishaw, 158 F.3d at 1248 ("[T]he claims define the scope of the right to exclude; the claim construction inquiry, therefore, begins and ends in all cases with the actual words of the claim...."). It is therefore both unfair and improper to graft unclaimed elements from the inventor's specification onto the claims because doing so cheats the patentee of intellectual property to which he or she is entitled by law. See Texas Digital, 308 F.3d at 1204 ("But if the meaning of words themselves would not have been understood to persons of skill in the art to be limited only to the examples or embodiments described in the specification, reading the words in such a confined way would mandate the wrong result and would violate our proscription of not reading limitations from the specification into the claims.")(emphasis added).

IV. THE LENGTH AND COMPLEXITY OF MICROSOFT'S PROPOSED CONSTRUCTIONS

Microsoft's proposed constructions are undoubtedly the longest and most complex claim constructions ever presented by a patent litigant. Microsoft's definition of VDE alone amounts to over 2,000 words, including numerous separately defined terms that are incorporated by reference.[3] That definition is over ten times longer than the longest proposed definition InterTrust can find in any Federal Circuit opinion. In fact, as best InterTrust can determine, Microsoft's definition is far longer than any claim construction ever proposed by any party in any patent litigation.

Although VDE is Microsoft's longest definition, it is not alone in its excesses: twelve of Microsoft's other definitions amount to over one hundred words each. Derwin Decl., ¶ 4. Many of these include multiple hundreds of words and incorporate other defined terms by reference.

InterTrust's patent claims are relatively straightforward. '721 Claim 34, for example, amounts to a total of 67 words. Microsoft's VDE definition by itself is more than thirty times longer than the entire claim, not to mention much more complex, yet Microsoft seeks to incorporate this mammoth definition into the claim despite the fact that the claim itself does not recite a VDE. If Microsoft's constructions were adopted wholesale, the jury instruction "explaining" this claim by itself would amount to at least 3,000 words, and probably many more.

No jury could possibly understand or apply constructions of this length and complexity. No jury has ever been asked to do so. Microsoft's proposals are designed to entirely defeat the purpose of claim construction, since they would render the claims far more difficult to

[3] Declaration of Douglas K. Derwin In Support of InterTrust's Claim Construction Position

understand, rather than less:

> [I]n the end, claim construction must result in a phraseology that can be taught to a jury of lay people. It is not enough simply to construe the claims so that one skilled in the art will have a definitive meaning. Control Resources, Inc. v. Delta Electronics, Inc., 133 F. Supp. 2d 121, 127 (D. Mass. 2001); see MacNeill Engineering Co., Inc. v. Trisport, Ltd., 126 F. Supp. 2d 51, 56 (D. Mass. 2001), dismissed on appeal; 2001 WL 838410 (Fed. Cir. 2001) ("The Court's 'claim construction obligation ... involves not only properly construing the claim language so that the litigants (for the most part skilled in the particular art) will understand it, but also teaching the chosen construction to the jury in language that will inform the jury in plain English the legal framework it must apply in order to do justice.'").

SKW Ams. v. Euclid Chem. Co., 231 F. Supp. 2d 626, 639 (N.D. Ohio 2002).

Definitions so long and complex as to defy meaningful application are per se unreasonable.

V. SPECIFIC CLAIM CONSTRUCTION ISSUES

This section sets forth a brief statement of InterTrust's position and supporting evidence, on each of the specific disputed claim terms.[4] By necessity, these explanations are abbreviated, and must be read in conjunction with the proposed claim constructions and supporting evidence contained in the Joint Claim Construction Statement ("JCCS"). Given the number of disputed terms, and the size and complexity of Microsoft's proposals, it is impossible within the page limits of this Memorandum for InterTrust to address all (or even a majority) of the specific issues raised by the Microsoft definitions. Instead, this Memorandum will describe evidence supporting InterTrust's constructions and will point out one or more significant problems with each Microsoft definition. For a more general overview, the accompanying Reiter Declaration includes an explanation of the background of the patents and of the claims as a whole, and may be consulted by the Court for an understanding of the context in which these claim elements

("Derwin Decl."), ¶ 3.

[4] Terms are listed in the order presented in the claims, using the same order as JCCS Exhibit A. The parties' proposed constructions can be found at the JCCS Exhibit A and Exhibit B locations cited below in the heading of each section. Evidence citations are to JCCS Exhibit C, unless otherwise noted. Such citations are given using the tab number from the Exhibit (each tab corresponding to a particular defined term), and a letter designating the particular quotation (e.g., 1(A) is a reference to Exhibit C, Tab 1 ("aspect") and in particular to the quotation designated as "A". References to Exhibit D are to items contained in the list of evidence submitted by Microsoft in Exhibit D to the JCCS.

appear. Reiter Decl., ¶¶ 5-17 and Ex. B.

The Court should not assume that InterTrust agrees with sections of Microsoft's proposed definitions that are not addressed herein. In general, the issues discussed below are exemplary of the vast majority of limitations improperly incorporated into the Microsoft definitions: those limitations either contradict the specifications, are completely unsupported, or attempt to transform preferred embodiments into claim limitations.

A. Global Requirement of a Virtual Distribution Environment (Ex. A, Row 1, Ex. B, Row 24, Ex. C, Tab 24)

Microsoft asserts that each and every claim requires a Virtual Distribution Environment ("VDE"), even though this phrase appears in only one of the twelve claims at issue, and even in that claim the phrase is only in the preamble. Microsoft's definition of Virtual Distribution Environment includes 690 words, and incorporates separately defined terms that bring the total to over 2,000 words of text. Microsoft thus asks the Court to read an extraneous 2,000 word definition into every single claim.

In the current section, InterTrust will discuss Microsoft's Global Construction position. Issues raised by the definition itself are discussed below, in Section Y.

1. The eleven claims other than 900.155[5] do not recite a "Virtual Distribution Environment" and do not contain any language implying any such requirement.

None of the eleven claims other than 900.155 includes any mention of a VDE. Moreover, none of those claims contains any language from which inclusion of a VDE limitation can be inferred. 193.1, for example, recites a method that can be performed by a single user: a music file is received, control(s) are used to determine if the music file can be copied to a second device (e.g., a portable music player); if the control(s) allow the transfer, the music file is transferred to the second device and the music is played through an audio output at that device. See Reiter Decl., Ex. B, p.1.

Compare this claim to Microsoft's definition of VDE. The first numbered paragraph of that definition is titled "Data Security and Commerce World," and describes a "multi-node world

[5] Claim 155 of the '900 patent.

(community)," recites guarantees provided to "all" participants, and expressly excludes "anything less than or different than this." The sixth numbered paragraph specifies that "each VDE node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, Clearinghouse, etc.)" The seventh numbered paragraph is titled "Comprehensive Range of Functions" and states that "VDE comprehensively governs (Controls) all security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts . . . ."

None of these elements has anything to do with the claim at issue. 193.1 does not require a "world," nor a multi-node community, nor guarantees to "all" participants. 193.1 does not mention or require content packagers, distributors or clearinghouses, nor does it have any language requiring or suggesting that "each" VDE node can play any role.

Similar points can be made relating to the other sections of the Microsoft definition. These and many other requirements from Microsoft's 2,000 word definition of VDE are completely irrelevant to 193.1, and equally irrelevant to the other claims at issue in this litigation. For example, 721.1 consists of 67 words, not one of which requires, implies or even relates to the VDE limitations Microsoft seeks to graft onto it. The absurdity of reading 2,000 additional words of limitation into a 67-word claim is obvious.

2. Incorporation of Virtual Distribution Environment into Claims Neither Reciting Nor Implying Such a Limitation Is Improper.

The evidence cited by Microsoft in Exhibit D to the JCCS indicates that Microsoft intends to argue that statements in the '193 and '683 patents regarding the "invention" compel reading all elements of a VDE into all claims. Although statements in an application regarding the "invention" may be taken into account in claim interpretation, neither the Federal Circuit nor any District Court has ever used such statements to read elements such as those proposed by Microsoft into all claims. Instead, the case law is clear that, under circumstances such as those presented in this case, statements in a patent's specification about the "invention" do not serve to limit the scope of issued claims.

a. The eleven claims other than 900.155 contain no limitations relating to a Virtual Distribution Environment.

According to the Federal Circuit, statements in an application regarding the invention cannot be read into the claims absent a relevant limitation in the claims themselves. For example, in Amgen Inc. v. Hoechst Marion Roussel, Inc., 314 F.3d 1313 (Fed. Cir. 2003), although the patent specification stated that, "the invention [was] 'uniquely characterized' by" a particular element in dispute, the asserted claims made no reference to that element, and the Federal Circuit held as follows:

> The statement that the invention is "uniquely characterized" by the expression of exogenous DNA sequences does not impel us to accept TKT's position when the asserted claims do not contain such an express limitation.

314 F.3d at 1326.

The Federal Circuit ruled similarly in Renishaw PLC v. Marposs Societa' Per Azioni, 158 F.3d 1243 (Fed. Cir. 1998):

> [I]t is manifest that a claim must explicitly recite a term in need of definition before a definition may enter the claim from the written description. . . .
>
> Thus, a party wishing to use statements in the written description to confine or otherwise affect a patent's scope must, at the very least, point to a term or terms in the claim with which to draw in those statements. Without any claim term that is susceptible of clarification by the written description, there is no legitimate way to narrow the property right.

158 F.3d 1243, 1248.

The eleven claims other than 900.155 do not recite a VDE. Nor do they include any other limitations that require one. Reiter Decl., ¶¶ 20-23.

b. Statements in the specifications do not clearly disclaim patentable subject matter, and therefore cannot be used to limit the claims.

The Federal Circuit has repeatedly held that, in order to limit the scope of a claim, specification statements about the "invention" must clearly and unambiguously exclude or disclaim certain embodiments. As noted, in Amgen the patent specification stated that, "the invention is 'uniquely characterized' by" a particular element. 314 F.3d at 1326. The Federal Circuit held, however, that this statement could not limit the claims: "Amgen's statements simply do not clearly indicate that exogenous expression is the only possible mode of the invention or that other methods were outside the stated purpose of the invention." 314 F.3d at 1334.

Likewise, in Honeywell Inc. v. Victor Co. of Japan, Ltd., 298 F.3d 1317 (Fed. Cir. 2002), the Federal Circuit held that, in order to be given effect as a claim limitation, "invention" language in the specification must constitute a "broad and unequivocal" disclaimer, such as an explicit statement in the specification that "all embodiments of the present invention" include a specific feature. 298 F.3d at 1325. See also Teleflex, Inc. v. Ficosa North America Corp., 299 F.3d 1313,1324 (Fed. Cir. 2002) (requiring "expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope"); Moore U.S.A., Inc. v. Standard Register Co., 229 F.3d 1091, 1111 (Fed. Cir. 2000) (references to the "present invention" or "aspects" of the "present invention" did not constitute claim limitations), cert. denied, 532 U.S. 1008 (2001).

The Federal Circuit has also held that specification statements about the importance of features or the intent to solve certain problems do not govern claim construction in the absence of express related language in the claims:

> [T]he fact that the claimed composition was designed to solve certain problems of the prior art and the fact that the patentee noted the functional import of having a homogeneous cast does not mean that we must attribute a function to the nonfunctional phrase "substantially uniform." Where the function is not recited in the claim itself by the patentee, we do not import such a limitation.

Ecolab, Inc. v. Envirochem, Inc., 264 F.3d 1358, 1367 (Fed. Cir. 2001).

The InterTrust specifications contain no language even remotely similar to the statement in Amgen that the invention was "uniquely characterized" by an element, a statement the Federal Circuit found insufficient to act as a binding limitation on all claims. The specifications contain no explicit disclaimers of any subject matter, nor are there any unambiguous (or even ambiguous) statements to the effect that all embodiments other than a complete VDE are outside the scope of the patents.

c. Specification statements about the "invention" are only one factor in claim interpretation, and must be interpreted in light of the entire specification and file history.

Specification statements about "the invention" must be read in light of the specification and file history as a whole, and such statements do not limit the claims if the rest of the specification and file history do not indicate that such a limitation was intended. Rambus Inc. v. Infineon Techs. Ag, 318 F.3d 1081, 1094-95 (Fed. Cir. 2003).[6]

In the present case, there are numerous aspects of the specification and file history that contradict Microsoft's argument that VDE must be read into all the claims.

(i) The Patent Office ruled that the parent InterTrust patent application involved five separate and independent classes of invention.

Although Microsoft would have the Court read the patent specifications as if they described a single "invention," and thereby read that "invention" into every single claim, the file history conclusively rebuts that argument. Not only did the Patent Office not find that the InterTrust specification described a single invention, it held that the parent InterTrust patent application claimed five separate **categories** of invention. It further held that these categories of invention each had "separate utility" separate and apart from any overall combination (e.g., a VDE). September 25, 1996 Office Action, pp. 2-3 (24(BB)). The Patent Office's ruling included the following text:

> 1. Restriction to **one of the following inventions** is required under 35 U.S.C. § 121:
>
> Group I . . . drawn to a secure component-based operating process, classified in Class 380, subclass 25.
>
> Group II. . . . drawn to method(s) for managing a resource or operating, classified in Class 380, subclass 4.
>
> Group III. . . . drawn to a secure method, classified in Class 380, subclass 3.
>
> Group IV. . . . drawn to [a] method of negotiating electronic contracts, classified in Class 364, subclass 401.
>
> Group V. . . . drawn to methods of auditing a resource, classified in Class 364, subclass 406.
>
> **The inventions are distinct, each from the other because of the following reasons:**
> 2. Inventions of Groups I-V are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention of Group I has separate utility such as protecting executable code from computer viruses. Invention of Group II has separate utility such as a computer network administration. Invention of Group III has separate utility such as protection of software. Invention of Group IV has separate utility such as a contract bidding procedure. Invention of Group V has separate utility such as auditing pay television. . . .

[6] InterTrust is providing a courtesy copy of the Rambus opinion as it appears on Westlaw.

> 3. Because **these inventions are distinct for the reasons given above and have acquired a separate status in the art** as shown by their different classification, restriction for examination purposes as indicated is proper.
>
> 4. Because **these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter**, restriction for examination purposes as indicated is proper.

24(BB) (emphasis added).

The Patent Office could hardly have been clearer: InterTrust's parent application involved five separate classes of invention. Each class of invention had utility separate from all of the others. Each class of invention was recognized in the art as relating to a divergent subject matter.

Based on this ruling, the Patent Office entered a "restriction" requirement, in which InterTrust was directed to pick one class of inventions to be pursued in the application. InterTrust did so, and also filed separate "divisional" applications relating to the other categories of inventions. Derwin Decl., ¶ 2.

Of the patents now at issue, '193, '891 and '912 have specifications identical to the original application, and correspond to three of the different invention categories identified by the Patent Office. The '900 is a continuation-in-part and also includes all of the text from the original application. Derwin Decl., ¶ 2. Thus, of the specification quotations cited by Microsoft in support of its VDE "global construction" argument virtually all were present in the original InterTrust application, the application determined by the Patent Office to involve five separate categories of invention.

The Federal Circuit has emphasized that divisional applications, such as those filed in this case, involve separate and independent inventions:

> A 'divisional' application, . . . is one carved out of an earlier application which disclosed and claimed more than one independent invention, the result being that **the divisional application claims only one or more, but not all, of the independent inventions of the earlier application.**

Transco Prods. Inc. v. Performance Contracting, 38 F.3d 551, 555 (Fed. Cir. 1994) (citing The Manual of Patent Examination Procedures, 1988 § 201.06) (emphasis added), cert. denied, 513

U.S. 1151 (1995).

The Rambus case cited above also involved a restriction requirement issued by the Patent Office, a factor noted by the Federal Circuit in its holding that statements regarding the "invention" could not be read into all claims. 318 F.3d at 1095.[7]

The Patent Office split the InterTrust patent application into five separate categories of invention. Microsoft now seeks to reverse that action, asking the Court to interpret the resulting patents as if they involved a single invention (VDE) and to read that "invention" into every single patent claim. Microsoft's position is directly contrary to the Patent Office's decision, a decision to which this Court is required to give,

> the deference that is due to a qualified government agency presumed to have properly done its job, which includes one or more examiners who are assumed to have some expertise in interpreting the references and to be familiar from their work with the level of skill in the art and whose duty it is to issue only valid patents . . . .

McGinley v. Franklin Sports, Inc., 262 F.3d 1339, 1353 (Fed. Cir. 2001).

(ii) Microsoft's interpretation of "the invention" is contradicted by the claims.

In Rambus, the Federal Circuit held that specification statements regarding "the invention" did not limit the claims. One factor it cited was the fact that the patentee had submitted some claims that expressly recited the element characterized in the specification as "the invention," thereby making it clear that the specification statements about "the invention" were not intended as a limitation on the claims in general, since otherwise the express inclusion of that element in other claims would have been redundant. 318 F.3d at 1095.

Exactly the same situation is present here. U.S. Patent No. 5,949,876 is an InterTrust patent issuing as a direct continuation from the original February 1995 patent application. It therefore includes the same specification as the '193 patent, including the same statements

[7] The Rambus discussion of the restriction requirement is not exactly parallel to the present facts, since at least one of the restrictions involved in that case apparently involved the exact claim limitation that was at issue, whereas none of the restrictions involved in the present case specifically mentions "Virtual Distribution Environment." It is indisputable, however, that the Patent Office in this case determined that multiple classes of invention were presented by the InterTrust applications, thereby contradicting any implication that specification references to "the invention" mean that all claims must be interpreted in light of a single invention.

regarding "the invention" and VDE that Microsoft has cited. The '876 patent includes numerous dependent claims adding an express requirement that a process or method include a VDE. 24(J). These dependent claims thus make it clear that claims that do **not** expressly recite a "Virtual Distribution Environment" were not intended to, and cannot be interpreted to include one.

B. Secure/Security (Ex. A, Row 3, Ex. B, Row 19, Ex. C, Tab 19).

Both parties acknowledge that the terms "secure" and "security" require some degree of protection against certain threats. InterTrust's proposed definition is consistent with the plain meaning of these terms as well as the patent specifications. It requires one or more mechanisms to prevent, detect, or discourage misuse of or interference with information or processes, and provides examples of the types of mechanisms that may be involved.

In contrast, Microsoft burdens these claim terms with numerous additional requirements that are inconsistent with both the ordinary meaning and the way these terms are used in the specifications. Two of these unwarranted additional requirements are addressed below.

1. Microsoft's requirement that five specified properties be protected.

Microsoft defines the word "secure" to require, in every instance, protection of five specified properties (availability, secrecy, integrity, authenticity and nonrepudiation). The specifications contradict this reading.

The specifications frequently use the words "secure" or "security" to refer to the use of one or more of a collection of protection mechanisms, without requiring the comprehensive protection of all of the properties specified by Microsoft. The following passage, for example, could hardly be clearer:

> In one embodiment, the portable appliance 2600 could support **secure (in this instance encrypted and/or authenticated)** two-way communications with a retail terminal which may contain a VDE electronic appliance 600 or communicate with a retailer's or third party provider's VDE electronic appliance 600.

'193 patent 233:25-30 (19(H) (emphasis added).

This passage describes "secure" in terms of encryption and/or authentication. These amount at best to two of the properties from Microsoft's list (secrecy and authenticity). No mention is made of availability, integrity or nonrepudiation. <u>See also</u> Reiter Decl., ¶ 28, discussing 19(A) ("security" referring to concealment and authentication), 19(B), ("secure" referring to concealment and authentication), 19(C) ("security" referring to concealment and tamper resistance), 19(D) ("security" referring to concealment and authentication), 19(E) ("security" referring to concealment, tamper resistance and access control), 19(F) ("secure" referring to concealment), 19(G) ("secure" referring to tamper resistance), 19(H) ("secure" referring to concealment and/or authentication), 19(I) ("secure" referring to concealment).

Microsoft's definition requires that all five specified properties be protected. As used in the specification, however, the term "secure" often means protection of fewer than these five properties. Microsoft's definition is inconsistent with the specifications and should be rejected.

2. Microsoft's requirement that "all users" be "guaranteed" protection against "all of the identified threats"

Microsoft's definition requires a guarantee to "all users" of absolute protection against all identified threats. This aspect of Microsoft's definition also contradicts the specifications, which make it clear that "secure" and "security" do not require absolute protection, but instead require only that security be sufficient for an intended purpose:

> The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, **and may vary widely**.

193 patent at 49:59-62 (19(J)) (emphasis added). See also 19(B) ("sufficient security (sufficiently trusted) for the intended commercial purposes"), 19(M), 19(N). The specifications also describe mechanisms used to limit the effects of a security breach, something that would be inconceivable if "security" or "secure" required absolute protection. See, e.g., 19(K), 19(L), 19(R), 19(S), 19(T).

Moreover, it is understood in the art that security can never be absolute. See, e.g., 19(BB) ("One hundred percent security cannot be achieved") 19(EE) ("security is a relative, not an absolute concept"), 19(X), 19(Y), 19(Z), 19(AA), 19(CC), 19(DD).

Microsoft's definition requires that absolute security be guaranteed to all participants and against all threats. This is inconsistent with use of this term in the specification, and with the universal understanding in the field, not to mention common sense. No one of ordinary skill in the art would interpret "secure" in this manner. Microsoft's construction is an attempt to define the term in a manner impossible for any real world system to attain. That construction should be rejected.

C. Budget (Ex. A, Row 4, Ex. B, Row 3, Ex. C, Tab 3).

In the specifications, "budget" is used consistently with its normal English meaning (3(A)), and InterTrust's definition of "information specifying a limitation on usage" reflects that meaning (3(L)). Microsoft similarly defines this term as referring to a "limitation on use," but then distorts this plain meaning into a budget "method," consisting of instructions and related data. The specifications, however, explicitly distinguish between a "BUDGET method" and the word "budget:"

> In the example shown in Figure 41d, a distributor at a VDE distributor node (106) might request budget from a content creator at another node (102). . . . The creator 102 may decide to grant budget to the distributor 106 and processes a distribute event (1452 in BUDGET method 1510 at VDE node 102). A result of processing the distribute event within the BUDGET method might be a secure communication (1454) between VDE nodes 102 and 106 by which a budget granting use and redistribute rights to the distributor 106 may be transferred from the creator 102 to the distributor. The distributor's VDE node 106 may respond to the receipt of the budget information by processing the communication using the reply process 1475B of the BUDGET method 1510. The reply event processing 1475B might, for example, install a budget and PERC 808 within the distributor's VDE 106 node to permit the distributor to access content or processes for which access is control at least in part by the budget and/or PERC.

'193 patent, 172:61-173:14 (3(C)) (emphasis added).

This passage is unmistakable: the word "budget" does not necessarily mean a "BUDGET method." A "BUDGET method" is a means to grant a "budget," but it is impossible to read this passage without understanding that the word "budget," by itself, does not mean "BUDGET method." See also 3(D) ("BUDGET method 408 may store budget information"), 3(E) ("BUDGET method" used to process "budget information").

Microsoft's citations from the specification indicating that a "budget" may be a type of method are not inconsistent with InterTrust's interpretation, since InterTrust agrees that a budget method is one possible embodiment of a budget. But that is all it is: one example of how a budget may be specified. Thus, item (1) from Microsoft's Exhibit D support for "budget" refers not to the word "budget" in general, but to, "'Budgets' 308 shown in FIG. 5B." The larger context for this passage is shown in 3(F), which makes it clear that the passage cited by Microsoft relates to one specific example of a budget, i.e., "Budgets 308" from Figure 5B, a figure that provides additional detail on the "preferred embodiment" shown in FIG. 5A, itself described as merely an "example." Reading preferred embodiments from the specification into the claims violates basic Federal Circuit claim construction principles. Laitram Corp. v. Cambridge Wire Cloth Co., 863 F.2d 855, 865 (Fed. Cir. 1988) ("References to a preferred embodiment, such as those often present in a specification, are not claim limitations."), cert. denied, 490 U.S. 1068 (1989).

Microsoft's definition also requires that a budget constitute a "decrementable numerical limitation." There is no basis in the specification (or the normal meaning of "budget") for any requirement that this constitute a "decrementable" value, as opposed to a value that is incremented until a limit is reached. Thus, a budget specifying that a user has the right to make three copies of content could be implemented as a decrementable value (starting with "3" and counting down each time a copy is made until "0" is reached) or as an incrementable value (starting with "0" and counting up until the value of 3 is reached). This is an implementation detail, and both types of value are supported in the specification. See, e.g., 3(H) (describing an "ascending use counter" and a "descending use counter.") There is no basis for limiting budgets to a decrementable value. This constitutes yet another Microsoft attempt to read a particular specification embodiment into the claims, an attempt that is particularly misguided in this case, since an alternate embodiment (an incrementable counter) is also disclosed.

D. Control (noun) (Ex. A, Row 4, Ex. B, Row 8, Ex. C, Tab 8).

Although the specification contains no explicit definition for "control," it does indicate that "rules and controls" are equated with "control information." See, e.g., 8(A), 8(B); see also 8(C) ("control" and "control information" used interchangeably).

Control information can consist of either programming (e.g., load modules) or data. See, e.g., 8(D) (load modules, data and methods), 8(F) (a key is control information), 8(G) (executable programming such as load modules), 8(H) (use of "and/or" making it clear that control information can consist of methods, or load modules, or mediating data or component assemblies), 8(I) (software and parameter data).

In the '193 and related file histories, prior art data items were repeatedly interpreted as constituting "controls." See, e.g., 8(W) ("control" read onto personal identification information), 8(X) ("control" read onto a list of checkwords), 8(Y) ("control" read onto password), 8(Z) ("control" read onto security code attribute indicating security levels).

Thus, "controls" can consist of various types of information, including programming (load modules, methods, component assemblies) and data. This is consistent with the InterTrust construction of the term.

The InterTrust construction also specifies that controls can govern operations on, or use of, resources (e.g., content), including permitted, required or prevented operations, the nature and extent of operations, and the consequences of operations. Again, this is consistent with use of the term control information in the specification. See, e.g., 8(J), 8(A), 8(H), 8(K), 8(L), 8(M), 8(B), 8(N), 8(O).

Microsoft's definition requires that controls be "executable." Although the parties disagree regarding the definition of "executable," neither party's proposed definition would include data. As is established above, however, the patents indicate that "controls" may include data. Microsoft's incorporation of "executable" into the definition of controls is therefore improper.

The Microsoft definition further requires that controls execute in a Secure Processing Environment ("SPE"). However, the patents make it clear that an SPE is a particular embodiment, and clearly disclose an alternate embodiment known as a Host Processing Environment ("HPE"), an embodiment excluded by the Microsoft definition. See Protected Processing Environment (§ P, below). The patents explicitly state that any operation that carried out by an SPE can also be carried out by an HPE. 16(D).

Microsoft's definition also requires the ability to modify controls. MS deft., ¶ (7). This is a preferred embodiment, and in any event is a capability provided by the ROS (an operating system described in the specification) rather than by the controls themselves. 8(Q).

Microsoft also seeks to apply the general definition of "control (n.)" to "user controls" as recited in 683.2. InterTrust objects to this, since "user controls" was a term on the parties' initial list of claim terms to be construed, but was not selected for the initial hearing, and InterTrust therefore requests that the Court reserve construction of this term.

Moreover, "user controls" in claim 683.2 is entirely unrelated to the "controls" discussed above. That sense of "control" is synonymous with "rules," and is a form of information that tells the system what the user may and may not do with the relevant content. By contrast, as used in 683.2, "user controls" refer to the hardware used to control a computer (such as a keyboard or mouse), rather than information or programming. In the claim, user controls are listed with other hardware elements (also including communications port, processor and memory). Significantly the digital information recited in the claim is explicitly identified as being stored in the memory (first secure container, governed item, first secure container rule, etc.), whereas "user controls" is listed as an element separate and apart from the memory. Moreover, in the file history the Examiner used a keyboard as an example of "user controls." 8(AA). Thus, the file history and the claim make it clear that "user controls" means something entirely different from either party's proposed construction of "control" as used in the other claims.

E. Copy/Copied/Copying (Ex. A, Row 5, Ex. B, Row 10, Ex. C, Tab 10).

InterTrust's proposed definition is the plain English meaning, based on "reproduce." This is consistent with the generally understood definition of this term. 10(K), 10(L), 10(M).

Microsoft's first sentence is consistent with InterTrust's construction, except for Microsoft's requirements that "all" of a file be reproduced and that this constitute a "complete physical block of data." The specification contradicts these requirements, since it explicitly uses the word "copy" to refer to a partial reproduction. 10(A), 10(B).

The definitions also differ in that InterTrust's definition requires that the copy be usable, whereas Microsoft's allows a copy to be ephemeral, unusable or inaccessible. MS deft., ¶ (3).

As used in the relevant claims (193.1, 193.11, 193.15, 193.19), the whole point of making a "copy" is to use it. Microsoft's definition, however, would define the word "copy" to include reproductions that are ephemeral, unusable and inaccessible, thus interpreting this term to include internal "phantom" reproductions made by the computer in the process of using a file.

As Dr. Reiter's Declaration explains, such temporary internal reproductions are automatically created by the computer for purposes of the computer's internal processing, and the user is never even aware of their existence. Reiter Decl., ¶¶ 34-40. For example, such reproductions are made every time a file is opened (e.g., a memo is brought up on a computer's screen), even though, from the perspective of the user, such actions have nothing whatever to do with making a copy of the file.

Defining such automatically-generated, unusable reproductions as "copies" leads to an absurd interpretation of the claims. For example, in 193.1, the user receives a budget specifying the number of "copies" that can be made of a file. If "copy" means internal, phantom reproductions, a portion of that budget would be used up every time the user made any use of the file, even if the user did not deliberately make a "copy," and even if the action did not result in anything the user would recognize as a "copy." Thus, a budget to make three copies of the file would be used up if the user opened the file three times, even if the user never created any permanent, usable copies at all. A user whose paid-for budget to make copies of a file was used up by merely opening the file is a user who would probably be looking for a good consumer-fraud attorney.

Even worse, if Microsoft's interpretation of "copy" is accepted, once the 193.1 budget to make copies was exhausted, the user would not only lose the ability to make actual copies, but would also lose any ability to even open the file, since the act of opening the file causes the creation of internal phantom reproductions. Thus, a user with a budget to make three copies of the file would be able to open the file three times, after which he or she would have no ability to make any other use of the file whatever.

Such an interpretation is absurd. 193.1 clearly contemplates the user receiving a budget to make deliberately-intended copies that the user (or someone else) can make use of. Interpreting "copy" so that the copy budget would be used up by internal phantom reproductions requires completely ignoring the context of the claim. See Reiter Decl., ¶¶ 34-40 and § F, immediately below.

F. Budget Specifying the Number of Copies Which Can Be Made of Said Digital File (Ex. A, Row 6, Ex. B, Row 25, Ex. C, Tab 25).

This claim phrase is straightforward. It incorporates two separately defined terms (Budget and Copies), but there is no reason to interpret it using anything other than its plain English meaning.

Microsoft's definition, on the other hand, incorporates requirements that are unsupported by the phrase and contradict the specifications.

(1) Microsoft requires that the budget state "the total number of copies (whether or not decrypted, long-lived, or accessible)." No such requirement is imposed by the claim term and, as is described above (see § E), this requirement makes no sense, since the budget would be exhausted by internal, "phantom" reproductions of no benefit to the user. See Reiter Decl., ¶¶ 34-40.

(2) The Microsoft construction also requires that "No process, user, or device is able to make another copy of the Digital File once this number of copies has been made." The specification, however, explicitly describes processes that can be used to "refresh" budgets, so that a budget that has been exhausted (e.g., reached zero) can be increased. See, e.g., 25(O) (describing the acquisition of "additional budgets if the user wishes to continue to use the traveling object after the exhaustion of the available budget(s)"), 25(P) ("Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget") 25(Q) ("clearinghouse may handle the end user's request for additional budget"). Microsoft's proposed addition of this limitation is thus directly contradicted by the specification.

G. Control (verb) (Ex. A, Row 7, Ex. B, Row 9, Ex. C, Tab 9).

"Control," used as a verb (e.g., "controlling") is not specially defined in the specifications. The InterTrust construction is based on the common English definition for the term (9(O)), a construction supported by the use of this term in the specification. Passages cited in Ex. C at 9(A), 9(B), 9(C), 9(D), 9(E) and 9(F), for example, use the verb form of "control" to refer to conventional hardware or software operations, that cause or prevent certain acts or events. Reiter Decl., ¶ 42.

Microsoft proposes a lengthy and highly complicated definition for this term, without any support whatsoever. The evidence cited by Microsoft contains no indication that the verb form of control is defined in any particular manner in the specification, and certainly does not support the lengthy and complex definition proposed by Microsoft. In fact, the majority of Microsoft's Exhibit D evidence for this term (Ex. D, Row 9) relates to the noun form of "control," and does not even mention the verb form.

Not only is the Microsoft definition unsupported by the specification, restrictions contained in that definition are actually contradicted by the specification. For example, Microsoft requires that a controlled action cannot otherwise be taken by any user, process or device. This restriction ignores the specification's discussion of alternate control structures, whereby an action not allowed by one control structure may be allowed by another. See 9(G), 9(H), 9(I), 9(J).

The Microsoft definition also requires the use of a VDE Secure Processing Environment. This ignores the specification's discussion of Host Processing Environments, identified as an alternative to the Secure Processing Environment embodiment. See Protected Processing Environment (§ P, below); see also 16(D) (HPE can carry out any operation carried out by an SPE).

H. Controlling the Copies Made of Said Digital File (Ex. A, Row 7, Ex. B, Row 26, Ex. C, Tab 26).

The relevant claim (193.1) itself further explains this element as follows: "if said copy control allows at least a portion of said digital file to be copied and stored on a second device." This further description, along with the separately defined incorporated terms, fully defines this element by making it clear that the copy control is used to determine whether a digital file may be copied to a second device. InterTrust's proposed construction is based on this straightforward, plain English interpretation.

Microsoft requires that the copy control operate within a VDE Secure Processing Environment. No such requirement is imposed by the claim, and the specification describes embodiments based on a Host Processing Environment, rather than a Secure Processing

Environment. See Protected Processing Environment, § P, below; see also 16(D).

The Microsoft definition requires that the copy control control "all copies of the *Digital File*." The claim contains no such requirement, but instead requires control over copies that are made, as opposed to all copies that exist. Microsoft's interpretation apparently would require that the copy control, operational at the first device, somehow control copies of the file at the source from which the first device received the file, including copies at other locations to which that source sent the file. In context, it is clear that the copy control need only govern copies made by the first device, not all copies that exist.

Microsoft further requires that all uses and accesses be prohibited except to the extent allowed by the copy control(s). This assertion has no support in the claim, and ignores the possibility that the item may also be governed by an alternate control structure. 26(A), 26(B), 26(C), 26(D).

I. Authentication (Ex. A, Row 27, Ex. B, Row 2, Ex. C, Tab 2).

This word is not specially defined in the specifications or the file histories. Both parties' proposed definitions focus on identifying something or someone.

The specification uses the term "authentication" to refer to various types of identification, including passwords (2(A), 2(B)), voice prints or retinal scans (2(B)) or certificates attesting that a device or key can be trusted. 2(C). InterTrust's proposed construction is consistent with these specification embodiments.

Microsoft's definition requires establishing that assertions about data integrity (i.e., that the data have not been altered) and origin integrity (i.e., confirming the source and time of origination) are genuine. In 193.15, however (the only relevant claim including this term), the word is used to describe a step involving an identifier associated with a device and/or user. Requiring "data integrity" and "origin integrity" makes no sense in the context of a user, and scarcely more sense in the context of a device. Moreover, none of the specification uses of this term implies such requirements.

The Microsoft definition is ambiguous regarding whether authentication requires uniquely identifying the person or thing authenticated. InterTrust's proposed definition, on the other hand, allows authentication to identify something or someone either as an individual or as a member of a group. This is supported by the specification, which describes an "Authenticate User" process that lets the caller authenticate a specific user ID or a group membership. 2(D).

J. Identifier (Ex. A, Row 28, Ex. B, Row 17, Ex. C, Tab 17).

The InterTrust definition is straightforward and consistent with the normal meaning of this term and with its use in the specification. <u>See</u>, <u>e.g.</u>, 17(A), 17(B).

The primary distinction between the parties' definitions concerns whether the identifier must be unique to an "individual instance" of a person or thing, or whether the identifier can specify that a person or thing is a member of a group.

In 912.8, this term is used in the following context:

> said load module including executable programming and a header;
>
> said header including an execution space **identifier** identifying at least one aspect of an execution space required for use and/or execution of the load module associated with said header;
>
>> said execution space **identifier** provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security;

A specification embodiment corresponding to this element is described in 30(A), in which a load module header is described as containing an "execution space code" that distinguishes SPEs from HPEs, with the explanation that some load modules are required to run in one type of environment as opposed to the other. This embodiment describes identifying an execution space as a member of a group (SPE or HPE) and therefore contradicts Microsoft's interpretation of "identifier" as requiring unique identification. Reiter Decl, ¶¶ 92-94.

Similarly, the specification uses the related terms "identification" and "ID" to refer to identification of an individual or a group. 17(D), 17(E). Thus, interpreting "identifier" as requiring a unique identification (as opposed to identification as a member of a group) would contradict the specification.

Microsoft also requires that an identifier constitute a "text string." No such requirement exists in the specification or any relevant claim. An identifier could constitute a string of numbers or bits (e.g., the retail terminal identifier described in 17(B), which might reasonably be expected to consist of numbers).

K. Clearinghouse (Ex. A, Row 40, Ex. B, Row 4, Ex. C, Tab 4).

The specification describes various embodiments of "clearinghouses," including entities that provide both financial and administrative services and may collect and distribute information. See 4(A), 4(B), 4(C), 4(D), 4(E), 4(F), 4(G), describing financial clearinghouses, document tracking clearinghouses, rights distribution clearinghouses, etc. InterTrust's proposed construction is straightforward, and describes these various embodiments.

Microsoft's construction, on the other hand, requires interpreting "clearinghouses" as limited to providing "store and forward" services. The specification, however, does not support limiting "clearinghouse" to this particular embodiment. Thus, Microsoft's Exhibit D quotations for this term describe other types of clearinghouses (e.g., financial clearinghouses) and none implies that a clearinghouse must provide "store and forward" services.

Nor do Microsoft's excerpts support any requirement that a clearinghouse operate under the constraints of "VDE security." The specification describes both Visa and AT&T as "clearinghouses." 4(B), 4(K). These are well-known organizations, and there is no suggestion in the specification that these organizations use "VDE security," nor would one of ordinary skill in the art so interpret these references. Reiter Decl., ¶ 48.

L. Use (Ex. A, Row 42, Ex. B, Row 23, Ex. C, Tab 23).

"Use" is a common English word, not specially defined in the specification and not a term of art. Reiter Decl., ¶ 49. InterTrust proposes giving the term its normal English meaning. See, e.g., 23(A).

Microsoft's proposed definition, by contrast, requires that "use" is allowed only through execution of controls. This is incorrect, since (a) controls include non-executable data (see Control, § D, above) and (b) the word "use" is a plain English word, with no technical meaning, and does not require or imply the use of any controls.

Notably, in the claims, when the "use" of an item is required to be governed by controls, this is explicitly set forth as a claim limitation:

> 683.2: securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item

Such claim limitations would be superfluous if the word "use" itself required the application of controls.

M. Secure Container (Ex. A, Row 57, Ex. B, Row 20, Ex. C, Tab 20).

The term "container" is not explicitly defined in the specification. The specification does, however, give numerous examples of containers that are consistent with InterTrust's proposed definition. 20(A). In addition, InterTrust's definition closely tracks the accepted definition of the term "container" in the computer field as of the relevant filing date. 20(J), 20(K). Note that such "containers" represent digital file formats, rather than physical containers.

The specification also contains no explicit definition of "secure container." InterTrust's definition of a Secure Container as a container that is "Secure" is simple, plain English, and is supported by the specification. 20(B), 20(C).

Microsoft's definition consists of approximately 290 words, including nine separately defined terms, many of which incorporate their own separately defined terms. Derwin Decl., ¶ 4. Such a definition is so long and complex as to render it impossible for the jury to understand or apply it.

Microsoft's definition also suffers from a number of specific defects, including the following:

(1) Microsoft requires that a secure container "cryptographically protects" information. MS deft., ¶ (1). Although the meaning of this statement is not entirely clear, it appears to require encrypting the secure container. The specification makes it clear that secure containers need not be encrypted (they can be "otherwise secured") and that protection need only be partial. 20(B).

(2) Microsoft requires that a secure container "encapsulates" its contents. MS deft., ¶ 1. This term is separately defined (in Microsoft's definition of Protected Processing Environment) as follows: "'Encapsulated' means hidden within an object so that it is not directly accessible but rather is accessible only through the object's restrictive interface."

The specification is clear, however, that the contents of a secure container are not necessarily "hidden within" the secure container but can be located externally, as long as the container contains a reference to the contents. 20(D), 20(E). Thus, a requirement that a secure container "encapsulate" its contents is inconsistent with embodiments disclosed in the specification.

(3) The last sentence of the Microsoft definition reads as follows:

> All **VDE**-protected information (including protected content, information about content usage, content-control information, **Controls**, and *Load Modules*) is encapsulated within a **Secure Container** whenever stored outside a *Secure Processing Environment* or secure database.

This statement is inaccurate (20(F)), but, in any event, it cannot constitute part of the definition of a "secure container," since it is not an attribute of a secure container and cannot be used by a trier of fact to determine whether a particular data structure does or does not constitute a "secure container." Instead, this passage describes the manner in which certain types of data are allegedly handled, rather than the properties of the secure containers themselves.

(4) Microsoft's definition requires that secure containers can only be opened in Secure Processing Environments. MS deft., ¶ (2). This ignores the specifications' disclosure of the alternate Host Processing Environment embodiment. See Protected Processing Environment, § P, below; see also 16(D).

(5) Microsoft requires that a secure container can only be opened through decryption of an encrypted header. MS deft., ¶ (2). The encrypted header, however, is described as a preferred embodiment, and therefore does not constitute a claim limitation. 20(G).

(6) Microsoft specifies that a container is not a secure container merely because it is encrypted and signed. MS deft., ¶ (5). The specification provides no support for such a statement, nor for any requirement that secure containers in fact be encrypted and signed. See, e.g., 20(B) ("encrypted or otherwise secured.")

N. Contain/Containing (Ex. A, Row 58, Ex. B, Row 7, Ex. C, Tab 7).

InterTrust's definition is based on the plain English meaning of this term. 7(C). This meaning is consistent with use of the term in the specification. See, e.g., 7(A).

The parties' definitions differ primarily in that InterTrust allows "contain" to include storing a reference or pointer indicating where an element may be found, whereas Microsoft excludes this. InterTrust's position is explicitly supported by the specification:

> . . . container 302 may "contain" items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites . . . .

7(B).

This passage, and established use in the field directly contradict Microsoft's definition of "contain" as excluding "addressing." 7(B); Reiter Decl., ¶¶ 51-59.

O. Aspect (Ex. A, Row 60, Ex. B, Row 1, Ex. C, Tab 1).

"Aspect" is not a technical term of art, and is not defined in either the specifications or the file histories. The term is used in its plain English sense throughout the relevant specifications. See, e.g., 1(A), 1(B), 1(C), 1(D), 1(E), 1(F), 1(G). InterTrust's proposed definition is consistent with these uses, and with the word's normal meaning.

Microsoft's proposed construction is limited to aspects of an "environment." This is inconsistent with the use of the term in 912.8 (aspect of an execution space), 861.58 (aspect of access to or use of secure container contents) and 683.2 (aspect of access to or use of a governed item). A construction inconsistent with the manner in which the term is used in the claims is obviously improper.

The Microsoft definition also requires a "persistent" element or property. The word "aspect" does not require or imply persistence. In one relevant specification, the word is used to refer to a feature that can be destroyed. 1(B). An "aspect" that can be destroyed is obviously an "aspect" that is not necessarily persistent.

P. Protected Processing Environment (Ex. A, Row 62, Ex. B, Row 18, Ex. C, Tab 18).

The InterTrust definition is closely tied to the description given for Protected Processing Environments ("PPEs") in the specifications (18(B), 18(C), 18(D)), as well as the manner in which PPEs are described in claims 721.34 and 683.2, each of which explicitly describes what is meant by the term.

The specifications describe two embodiments of PPE: a Secure Processing Environment

("SPE"), using a special-purpose microprocessor with hardware-based security (a "Secure Processing Unit") and a Host Processing Environment ("HPE"), using software-based security instead of a Secure Processing Unit. 18(B), 18(D), 18(E). InterTrust's proposed construction covers both embodiments, as is proper, since the specification explicitly states that any action that can be taken by an SPE can also be taken by an HPE, albeit possibly with a lower level of security. 16(D). A number of Microsoft's definitions, however, would improperly exclude the HPE embodiment (see, e.g., §§ F, G, H, M, X, Y, DD, above and below).

Microsoft's definition of PPE is considerably longer than the Gettysburg Address. It contains approximately 345 words in six numbered sections, as well as eleven separately defined incorporated terms, adding hundreds of additional words. No jury could possibly apply such a definition in any meaningful way.

Given the massive number of limitations Microsoft imposes on this term, a comprehensive rebuttal would require many pages. Several points, however, are worth noting:

(1) Microsoft states that "most" PPEs are Secure Processing Environments incorporating a Secure Processing Unit. MS deft., ¶ (2). Microsoft does not explain what the other PPEs are, though the Microsoft definition implies that they fall within the following description: "[a] facility employing physical facility and user-identity **Authentication** security procedures trusted by all **VDE** nodes, and the **VDE** node does not Access or **Use** VDE-protected information, or assign VDE control information." MS deft., ¶ (5).

As is described above, PPEs incorporating software-based security are known as Host Processing Environments ("HPEs"), and the specification states that HPEs can perform any function performed by an SPE. 16(D). Microsoft's apparent argument that HPEs are used only in clearinghouses and other physically secure facilities is contradicted by the specifications, which describe the use of HPEs for end users (18(H)) and in other contexts not involving clearinghouses. 18(I), 18(K).

(2) Microsoft requires that a PPE protects "all information identified in the patent application as being protected." To the extent that this requirement is not entirely circular (i.e., PPEs protect the information that is protected by PPEs), it appears to imply that all information

described in the patents as being protected by any mechanism must also be protected by PPEs. The specifications contain no support for any such requirement.

(3) The Microsoft definition states that certain PPEs may "be formed by a general-purpose CPU that executes all VDE 'security' processes in protected (privileged) mode." MS deft., ¶ (5). No support exists for the protected (privileged) mode restriction. See Host Processing Environment (§ Z, below).

Q. Digital Signature/Digitally Signing (Ex. A, Row 66, Ex. B, Row 14, Ex. C, Tab 14).

Although "digital signature" is not defined in the specification, this is a term of art widely used in the computer security field to refer to information that can be used to determine the source and/or integrity of a digital file. Reiter Decl., ¶ 62; 14(G). The term "digital signature" is used in the specification in a manner consistent with the InterTrust construction. 14(A), 14(B).

Microsoft's definition requires that a digital signature be "computationally unforgeable." Neither the specification nor any evidence cited by Microsoft requires any such absolute degree of protection.[8]

R. Designating (Ex. A, Row 66, Ex. B, Row 12, Ex. C, Tab 12).

This term is not specially defined in the specifications or file histories. InterTrust's proposed construction is based on the normal English meaning (12(F)), and in the specification the term is used in accordance with its normal English meaning. 12(A), 12(B), 12(C), 12(D), 12(E).

Microsoft requires that designating involve "restricting" something to a particular use. Neither the English meaning of this term nor the specification supports this limitation. To the extent that restricting to a particular use is required, this is an aspect of the overall claim in which this term is used (721.1), and is not inherent in the word "designate." Microsoft has identified no evidence in support of its construction. None exists.

[8] Microsoft's definition of "digital signature" includes a separate definition for the term "key." The parties dispute the correct definition of "key." This dispute is not relevant to "digital signature," and therefore is not discussed herein. The meaning of "key" is, however, important in other contexts, and InterTrust respectfully requests that the Court refrain from explicitly defining "key" at this time, as it is not one of the 30 terms selected for construction.

S. Device Class (Ex. A, Row 66, Ex. B, Row 13, Ex. C, Tab 13).

This term was explicitly defined in the file history, using the same definition InterTrust now proposes. 13(A). Such a file history definition is binding. Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("Although words in a claim are generally given their ordinary and customary meaning, a patentee may choose to be his own lexicographer and use terms in a manner other than their ordinary meaning, as long as the special definition of the term is clearly stated in the patent specification or file history.")

Microsoft cites no support from the specification for its proposed construction of this term. That construction is apparently based entirely on the manner in which this term is used internally at IBM, with no support for applying that construction to the InterTrust patent claims.

T. Tamper Resistance (Ex. A, Row 67, Ex. B, Row 21, Ex. C, Tab 21).

"Tamper resistance" is not explicitly defined in the specifications. The definition of this term, however, should follow from the stipulated definition of "Tampering" (JCCS Ex. I), as InterTrust's definition does. InterTrust's construction is also consistent with the use of this term in the specifications and in relevant extrinsic evidence. 21(A), 21(B), 21(C), 21(D), 21(E).

Microsoft states that "tamper resistance" requires a "tamper resistant barrier." Although 721.34 recites a "tamper resistant barrier," other claims reciting tamper resistance do not. For example, 900.155 specifies "tamper-resistant software" with no requirement of a barrier.

Microsoft requires that access, observation and interference be **prevented**. The term is not, however, tamper **prevention**, but tamper **resistance**, thereby clearly implying that some degree of resistance less than prevention would be sufficient.

Microsoft also requires that all access, observation **and** interference be prevented. Tamper resistance should be defined as resistance to Tampering, a separately defined term. By failing to incorporate this separately defined term, Microsoft requires that Tamper Resistance protect against actions that do not constitute Tampering (e.g., the definition of Tampering does not include any reference to "access.")[9]

[9] Microsoft repeats the definition of "tampering" in its construction of Tamper Resistance, but inexplicably fails to use that definition in defining Tamper Resistance.

U. Digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class (Ex. A, Row 67, Ex. B, Row 27, Ex. C, Tab 27).

InterTrust's proposed construction is a straightforward explanation of the phrase, consistent with the embodiment disclosed in the specification. 27(A), 27(B), 27(C), 27(D), 27(E), 27(F), 27(G). Microsoft's definition, on the other hand, builds in a variety of restrictions that are unsupported by the specification:

(1) Microsoft's definition requires that the digital signature be used "as the signature *Key*." As described at Reiter Decl., ¶¶ 63-64, a key may be used in a process that creates a digital signature, but the key and the signature are different things, one used in the process, the other the result of the process. Dr. Reiter has never heard of a digital signature used as a key to create a signature, and one of skill in the art would not interpret this phrase to imply any such requirement. Reiter Decl., ¶¶ 65-66. Neither the claim nor the specification, nor any evidence proffered by Microsoft supports such a bizarre reading of the phrase.

(2) Microsoft's definition also requires that "No VDE device can perform any execution of any *Load Module* without such authorization." The claim includes no such requirement, and this is irrelevant to interpretation of this element, since the claim simply requires that two particular load modules be digitally signed, and does not discuss signing of load modules in general.

(3) Neither this claim phrase nor the entire claim nor the specification as a whole require or support reading the concept of "VDE device" into this claim, as Microsoft's definition would require.

(4) Microsoft requires that the tamper resistance and security levels be persistent. Neither the claim nor the specification supports any such requirement.

V. Tamper Resistant Barrier (Ex. A, Row 71, Ex. B, Row 22, Ex. C, Tab 22).

The term "Tamper Resistant Barrier" should be defined in terms of Tamper Resistance. InterTrust's definition does so, and is consistent with use of the term in the specification (e.g., 22(C)). InterTrust's definition makes it clear that such a barrier may consist of hardware or software, as is required by use of the term in the specification. 22(B).

The Microsoft definition requires that a Tamper Resistant Barrier be an "active device." This is not supported in the specification, and "device" implies hardware, though the specification states that a tamper-resistant barrier can consist of software. 22(B).

Much of Microsoft's definition appears to be taken more or less verbatim from a description of hardware-based tamper resistant security barrier 502, as described in the specification. 22(A). This ignores software tamper resistant barriers, which are also described in the specification, but without the requirements imposed by hardware barriers (e.g., software tamper resistant barriers are less secure than hardware barriers). 22(B). Microsoft's definition therefore improperly limits the claims to one particular disclosed embodiment and entirely ignores a different disclosed embodiment.

W. Executable Programming/Executable (Ex. A, Row 73, Ex. B, Row 15, Ex. C, Tab 15).

Microsoft requires that an "executable" consist exclusively of machine code instructions. InterTrust's definition would include machine code versions of programs, but also includes programs written in higher-level languages that require "interpretation," which means the translation of a program into lower-level machine code instructions. Reiter Decl., ¶¶ 68-70.

The specification is clear that "executable" can refer to either lower-level machine code instructions or higher level instructions that have to be interpreted. See 15(A) (preferred embodiment is "native" instruction set (i.e., machine code), but an "interpreted" solution (i.e., higher level language) may also be used). Reiter Decl. ¶¶ 72-75. See also 15(B), which uses "executable" to refer to programs written in languages such as Java, a higher-level language requiring interpretation before being run. Java programs do not constitute machine code. Reiter Decl., ¶ 71.

InterTrust's definition is also consistent with the definition from the Microsoft Computer Dictionary. 15(C); Reiter Decl., ¶¶ 76-78.

Microsoft requires a "complete series of definitions and instructions," thereby implying an entire computer program. Although computer programs are made up of programming, the term "programming" by itself can mean an entire computer program or merely a portion. Reiter Decl., ¶ 79.

X. Securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item (Ex. A, Row 85, Ex. B, Row 28, Ex. C, Tab 28).

The term "securely applying" is not specially defined in the specification and is not a term of art. In the specification, the terms "securely applying" and "applying" refer to the application of control information to govern content. 28(A), 28(B), 28(C), 28(D), 28(E). This is consistent with InterTrust's proposed construction.

(1) The Microsoft definition requires use of a Secure Processing Unit. This ignores the alternate-embodiment HPE, which does not involve use of a Secure Processing Unit. <u>See</u> Protected Processing Environment, § P. Moreover, the claim itself recites a "secure operating environment," and the specification states that a secure operating environment can be either an SPE or an HPE. 28(H). Thus, requiring that this element take place using a Secure Processing Unit contradicts the proper interpretation of the claim, which the secure operating environment recited in the claim can consist of either an SPE or an HPE.

In addition, the specification uses "securely" to refer to operations taking place in either an SPE or an HPE. 28(F). Thus, this word does not imply any requirement of a Secure Processing Unit.

(2) Microsoft's definition of "securely applying" requires executing controls. Controls, however, include non-executable data (<u>see</u> Control, § D, above), and the specification uses the term "apply" to relate to applying data (non-executable). 28(G).

(3) Microsoft's definition requires that the resource constitute a component part of the appliance's secure operating environment. The claim imposes no such requirement, and there is no support for this requirement in the specification or anywhere else.

(4) The Microsoft definition requires that this action "governs all use of the data item by all users, processes, and devices." This limitation is not required by the claim and does not take into account embodiments describing alternative control structures, in which a use not allowed

by one control structure (e.g., a control) might be allowed by a different control structure. See Control, § D, above.

Y. Virtual Distribution Environment (Ex. A, Row 86, Ex. B, Row 24, Ex. C, Tab 24).

Microsoft's Global Construction argument is discussed above. This section will discuss Virtual Distribution Environment as the term is used in 900.155, the only claim at issue that actually includes this phrase.

"Virtual Distribution Environment" is used only in the preamble of the claim. The individual elements of 900.155 fully define the recited apparatus, and reference to the preamble is not necessary to define and understand the claimed apparatus. Reiter Decl. ¶ 80. Under such circumstances, the preamble does not "give life, meaning and vitality" to the claim and is irrelevant to claim interpretation. Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1371 (Fed. Cir. 2003),[10] Alfred J. Schumer v. Laboratory Computer Systems, Inc., 308 F.3d 1304, 1310 (Fed. Cir. 2002).

Assuming, arguendo, that this phrase needs construction, InterTrust's definition is taken directly from embodiments of virtual distribution environments described in the specification. 24(A), 24(B), 24(C). Microsoft's definition, on the other hand, is so long and complex as to defy thorough analysis, at least in the context of the page limits applied to this brief. Nevertheless, certain broad points can be made.

(1) Asking a jury to attempt to comprehend 900.155 by applying a 2,000 word definition would be asking the impossible. A definition of this length and complexity cannot clarify interpretation of the claim, but can only lead to confusion.

(2) Microsoft's definition requires an SPE. The specification clearly describes use of an alternate embodiment HPE. See Protected Processing Environment, § P, above.

(3) Microsoft's definition incorporates features that would necessarily be "universe-wide," and could not apply to any particular computer or group of computers, nor to any process performed on any particular computer or group of computers. Microsoft makes no attempt to

[10] InterTrust is providing a courtesy copy of the Altiris opinion as it appears on Westlaw.

explain how this "universe-wide" feature of VDE could be applied to a claim relating to a single device or process. For example, would determining whether a single device infringes a claim (e.g., whether a particular computer infringes 900.155) require analysis of the entire "universe" of devices? Such an analysis is obviously impossible and would render this and other claims a nullity.

(4) Microsoft's definition requires that a VDE "guarantees" various types of security, and that a VDE is "non-circumventable." Guaranteed security is impossible in the real world, and is not required by the specification. See 24(K) through 24(N), 24(P) through 24(AA).

Z. Host Processing Environment (Ex. A, Row 87, Ex. B, Row 16, Ex. C, Tab 16).

The two parties are in agreement that a Host Processing Environment ("HPE") is distinct from a Secure Processing Environment ("SPE"), and that an HPE may include software running on a general-purpose microprocessor.

Microsoft is correct that HPEs may be either "secure" or "non-secure." InterTrust's proposed definition is more accurately a definition of secure HPE, but not of a non-secure HPE. If need be, InterTrust's definition can be qualified to make it clear that an HPE may be either secure or non-secure, with the present definition applying to the secure version, and the non-secure version described as "a processing environment with insufficient security to constitute a secure HPE." Such a definition is consistent with use of this term in the specification. 16(A), 16(B), 16(C), 16(D), 16(E).

Microsoft's definition, however, incorporates numerous additional restrictions that are either unsupported by or contradicted by the specification.

(1) Microsoft implies that a HPE consists only of executable programming. This contradicts 900.155, which identifies various hardware elements as part of the HPE (e.g., a central processing unit, memory, etc.). This also contradicts Microsoft's construction of the claim phrase in which host processing environment appears ("Derives information from one or more aspects of said host processing environment"), since in that construction Microsoft requires that the host processing environment include hardware.

(2) Microsoft requires that a HPE be within a "VDE node." The Microsoft definition of

VDE incorporates several pages of detailed requirements, none of which is required by the manner in which HPEs are described in the claim or the specification. Issues regarding whether VDE should be read into every claim should be resolved in connection with Microsoft's "Global Construction" argument, discussed above, and should not be "back-doored" into the claims through the definition of specific terms.

(3) Microsoft's definition of "secure" HPE requires software running in "protected (privileged) mode" and that a non-secure HPE be running in "user mode." The specifications contain no discussion stating or even implying any such requirement. While the specifications do discuss processors running in "protected" or "privileged" mode, these discussions have nothing to do with (and do not mention) HPEs. 16(E), 16(F), 16(G), 16(H).

AA. Derive (Ex. A, Row 92, Ex. B, Row 11, Ex. C, Tab 11).

This is not a term of art and is not specially defined in the specification, in which it is used in its normal English sense. 11(A), 11(B), 11(C). InterTrust's proposed construction is based directly on the normal English definition. 11(E).

Microsoft defines "derive" to mean "retrieve from a source." That "derive" is not limited to retrieval from a source is made clear by use of the term in the specification 11(D) and by the embodiment disclosed for the phrase from 900.155 in which the term "derive" is used, an embodiment that clearly contemplates generating information. Reiter Decl., ¶ 86. This is plain English: when one "derives a conclusion," one generates information by the application of reasoning to facts. One does not simply "retrieve" the conclusion from storage.

BB. Derives information from one or more aspects of said host processing environment (Ex. A, Row 92, Ex. B, Row 29, Ex. C, Tab 29).

InterTrust's construction interprets this phrase in accordance with the plain English meaning of its words.

Microsoft requires that information be derived from the host processing environment "hardware." No such requirement is imposed by the claim, which specifies merely an "aspect" of the host processing environment. The disclosed embodiment reveals using software (e.g., the ROM BIOS, which constitutes software) and stored "information" for this purpose. 29(A);

Reiter Decl., ¶¶ 84-85. Moreover, this contradicts Microsoft's definition of host processing environment, since that definition requires that a host processing environment be made up of programming, rather than hardware.

Microsoft requires that the information "uniquely and persistently" identify the host processing environment. The claim includes no such requirement, stating only that the information be derived from "aspects" of the host processing environment, a term used to refer to features that may disappear. See Aspect, § O, above.

CC. Compares/Comparison (Ex. A, Row 94, Ex. B, Row 5, Ex. C, Tab 5).

These terms are not specially defined in the specification, but are used in accordance with their normal English meaning. See, e.g., 5(A), 5(B), 5(C), 5(D).. InterTrust's definition is based on that normal meaning.

Microsoft attempts to import additional limitations to this term, defining "compare" as limited to one particular type of microprocessor operation. The specification, however, does not discuss or even mention any such operation, and uses the word "compare" in its normal English sense, with no implication that a particular microprocessor operation is contemplated. 5(A), 5(B), 5(C). One of ordinary skill in the art would not understand "compare" to refer to one particular type of microprocessor operation absent a clear reason to do so. Reiter Decl., 87-89.

DD. Component Assembly (Ex. A, Row 99, Ex. B, Row 6, Ex. C, Tab 6).

InterTrust's proposed definition is taken directly from the manner in which the term is used in the specification and file history. 6(A), 6(B), 6(K).

Microsoft's definition requires that component assemblies be "created by a channel." The channel mechanism, however, is a preferred embodiment, not a claim element. 6(C).

The Microsoft definition requires that a component assembly include load modules. Although component assemblies may include load modules, the specification describes this as a preferred embodiment and describes load modules as merely an example of component assembly components. 6(D), 6(E) (note use of "e.g."), 6(F) (note use of "e.g.").

The Microsoft definition requires that a component assembly be assembled and executed in a Secure Processing Environment. This is directly contradicted by the specification. See 6(B) (component assemblies may be assembled, loaded and executed in either an SPE or an HPE); 6(G) ("certain" component assemblies require a secure execution space). See Protected Processing Environment (§ P), for an explanation of the differences between the SPE and HPE embodiments.

EE. Identifying at least one aspect of an execution space required for use and/or execution of the load module (Ex. A, Row 103, Ex. B, Row 30, Ex. C, Tab 30).

InterTrust's definition is based on the plain English meaning of this phrase, including the separately defined terms. Microsoft incorporates numerous limitations that are inconsistent with the specification and claims.

(1) The Microsoft definition requires that an execution space without "all of those required aspects" is "incapable of making any such Use (e.g., **Copying**, displaying, printing) and/or execution of the load module." This implies that, if the execution space lacks these required aspects but is still capable of making one of the recited uses, the claim element is not met. The element, however, specifies that the execution space identifier identify an execution space required for use "and/or" execution of the load module. Thus, if the load module can be "used" without being "executed," the claim limitation is still met.

(2) Microsoft requires that the identifier define "fully, without reference to any other information." No support exists for this in the claim or the specification, and the disclosed embodiment is inconsistent with this. Reiter Decl., ¶¶ 91-98.

(3) Microsoft's definition includes the following: "used to distinguish it from other environments of an **execution space**." This phrase has no obvious meaning.

//

//

//

VI. CONCLUSION

InterTrust's claim constructions rely on the straightforward plain English meaning of the claim terms, informed by the teachings of the specifications. Microsoft's constructions contradict the specifications in many respects, and attempt to incorporate numerous limitations taken directly from preferred embodiments. Moreover, Microsoft's definitions are far longer and more complex than any patent claim definitions ever adopted by any Court. No jury could possibly use those definitions in any meaningful way.

Microsoft's convoluted and confusing claim constructions are not based on the plain meanings of the terms, nor on the fundamental legal principles of claim construction. Instead, Microsoft can only avoid infringement if the InterTrust claims are so loaded up with extraneous detail that they become impossible to apply to any real world product or process. In doing so, Microsoft violates fundamental and settled Federal Circuit principles of claim construction, including the prohibition against reading embodiments from the specifications into the claims.

For the reasons set forth above, InterTrust respectfully requests that the Court adopt the constructions proposed by InterTrust.

Dated: March 17, 2003

DERWIN & SIEGEL, LLP

By:

DOUGLAS K. DERWIN
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

PROOF OF SERVICE

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

On March 17, 2003, I served the following document(s):

INTERTRUST'S OPENING CLAIM CONSTRUCTION BRIEF;

DECLARATION OF DOUGLAS K. DERWIN IN SUPPORT OF INTERTRUST'S OPENING CLAIM CONSTRUCTION BRIEF

DECLARATION OF DR. MICHAEL REITER IN SUPPORT OF INTERTRUST'S CLAIM CONSTRUCTION POSITION

DECLARATION OF MICHAEL H. PAGE IN SUPPORT OF INTERTRUST'S OPENING CLAIM CONSTRUCTION BRIEF

☑ by **FEDERAL EXPRESS**, by placing a true and correct copy in a sealed envelope addressed as shown below. I am readily familiar with the practice of Keker & Van Nest, LLP for correspondence for delivery by FedEx Corporation. According to that practice, items are retrieved daily by a FedEx Corporation employee for overnight delivery, and by E-MAIL.

Eric L Wesenberg, Esq.
Mark R. Weinstein, Esq.
Orrick Herrington & Sutcliffe
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650/614-7400
Facsimile: 650/614-7401

John D. Vandenberg, Esq.
James E. Geringer, Esq.
Kristin L. Cleveland, Esq.
Klarquist Sparkman Campbell, et al.
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland OR 97204
Telephone: 503/226-7391
Facsimile: 503/228-9446

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on March 17, 2003, at San Francisco, California.

DAWN CURRAN

MHP
94K

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
KENNETH J. HALPERN (State Bar No. 187663)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

MICROSOFT CORPORATION, a Washington corporation,

Counterclaimant,

v.

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Counter-Claim-Defendant.

Case No. C 01-1640 SBA (MEJ)

MICROSOFT'S BRIEF IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT THAT CERTAIN "MINI-*MARKMAN*" CLAIMS ARE INVALID FOR INDEFINITENESS

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

TABLE OF AUTHORITIES

FEDERAL CASES

TABLE OF CONTENTS

I. INTRODUCTION

The InterTrust patent claims' use of the vague term "secure" and its variants makes them textbook illustrations of the danger of indefinite claims. Without a definition of this malleable core term, persons of skill in the art cannot determine the scope of patent coverage. This is precisely the situation prohibited by 35 U.S.C. § 112's requirement of "particularly pointing out and distinctly claiming" the alleged invention. The purpose of the claims is to define the metes and bounds of the exclusive right that the public grants in exchange for the patentee's full disclosure. Where those boundaries are blurry, others are deterred from entering the field, allowing the patentee to exclude competition beyond the scope of the claimed invention. The InterTrust patent claims using "secure" and its variants violate the bargain with the public in this fashion, and should be found fatally indefinite and, therefore, invalid.

InterTrust's testifying expert concedes that "security" is an "essential aspect" of the "invention," InterTrust's so-called "Virtual Distribution Environment" ("VDE"). Declaration of Eric L. Wesenberg, Ex. A, Reiter Depo., 23:21-24:9.[1] "Secure," or some close derivative thereof, appears in virtually every disputed claim. Reading Claim 1 of U.S. Patent No. 5,892,891 ("the '891 patent") demonstrates the extensive use of the vague term "secure":

> A method for using at least one resource processed in a secure **operating environment** at a first appliance, said method comprising: **securely receiving** a first entity's control at said first appliance, said first entity being located remotely from said operating environment and said first appliance; **securely receiving** a second entity's control at said first appliance, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and **securely processing** a data item at said first appliance, using at least one resource, including **securely applying**, at said first appliance, through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item. (Emphases added.)

Ex. P, Claim 1. This claim uses four different, and five total, instances of this term or its variant. Neither the claims nor the rest of the patents define what it means for something to be "secure" or to be done "securely." "Secure," in the art, is a highly general, relative and multifaceted term

[1] Hereinafter, all cites to exhibits ("Ex.") are to exhibits attached to the Declaration of Eric L. Wesenberg in support of Microsoft's Motion for Summary Judgment that Certain "Mini-*Markman* Claims are Invalid for Indefiniteness.

which, without more specific definition, fails to have a clear or even useful meaning. In all their hundreds of pages of single-spaced description, the patents never clearly or consistently define "secure," nor the composite terms using secure (*e.g.*, "secure container"), nor the related coined terms deriving from the same concept: "protected processing environment" and "host processing environment."

The extrinsic evidence – both testimonial and documentary, both Microsoft's and InterTrust's – is in complete agreement: "secure" corresponds to a general concept in the computer field, which lacks specific meaning and standing alone may apply to numerous specific scenarios depending on the properties to be "secured," the particular threats posed, the means used, the degree of protection needed, the perspective from which one views "security," and so on.

Both parties' experts have testified that "secure" can take on a definite meaning within the context of a "security policy," which defines the parameters and sets objective criteria for determining whether they have been satisfied. Computer scientists have developed a number of models for objectively evaluating the security of different systems and architectures, at least one of which is mentioned (TCSEC), but not employed, in InterTrust's '193 patent.[2] InterTrust could easily have defined a security policy using any of these models. Instead, it left "secure" inscrutable throughout the patents.

The problem is not that it's difficult to discern the true meaning of these claim terms. It is impossible. For the reasons set forth herein, Microsoft asks that the Court find the claims containing "secure" (including its variants), "protected processing environment" or "host processing environment" invalid for indefiniteness.

///

///

///

[1] For efficiency, all references to "the specification" are to the specification of U. S. Patent No. 6,253,193 ("the '193 patent") (Ex.Q). The '193 specification reproduces, nearly identically, the "big book" original application (the original 900+ page application filed in 1995). Each of the patents at issue herein either expressly reproduce the same text in their specifications, or attempt to incorporate it by reference (though not successfully, *see infra* § II. D.).

II. FACTS

A. "Secure" Lacks a Clear Meaning in the Art.

The most pervasive indefinite term in the InterTrust patents is "secure" in all its various forms. Indeed, the provision of "security" while enabling the flexible distribution of digital information is the stated goal of the entire invention. To construe "secure," the Court must look to the ordinary meaning (if one exists) that would be attributed to the term by a person of skill in the art. *Tex. Digital Sys. v. Telegenix, Inc.*, 308 F.3d 1193, 1202 (Fed. Cir. 2002). The intrinsic and extrinsic evidence, including InterTrust's own statements and those of its expert, establish that while communicating a general or conceptual meaning, the term "secure" lacks a any precise, uniform definition to inform a person of skill in the art what it means unless a number of questions are answered. Because InterTrust never provides the needed answers, it is impossible to determine the scope of the claims.

"Secure memory" for instance, is no clearer a phrase than a "secure car." At first blush, one hearing the phrase "secure car" might think of a car equipped with features that make it difficult or impossible to steal, such as a club, an alarm siren, and or an ignition "kill switch." Only later in the conversation, hearing the speaker refer to bulletproof glass, shielded wheels, and reinforced doors would the listener realize that "secure" means something entirely different: The car is in fact designed to protect passengers from attack (to transport diplomats and heads of state). Even after the type of security is identified, different particular combinations of security measures will qualify the car as "secure" in the eyes of different customers. Simply referring to a car as "secure" fails to delineate the objective of that security, the type of security needed or the measures used to achieve it. Nor does the descriptor "secure" disclose the perspective from which "security" is being assessed. A parking enforcement officer might consider a booted vehicle "secure" (*i.e.*, from removal by its owner), while the owner might view it as "insecure" since it allowed someone to tamper with its wheels. Another variable might be the length of time the car would have to withstand the measures it is designed to resist. From this simple metaphor, the relative, multifaceted and undefined character of "secure" is readily apparent.

What is true in the vernacular applies with even greater force in the computing arts – "secure" needs definition along multiple axes to have a precise meaning. Deponents skilled and experienced in the field have spoken on this point. InterTrust's own expert, Dr. Michael Reiter, testified that "'secure' is a fairly general term that's used in the art for -- in several different ways." Ex. A, Reiter Depo., at 30:11-19. Asked to describe them, Dr. Reiter responded, "Oh, my gosh. All the ways. I can enumerate several ways I can think of on the fly. I don't know that I can enumerate everything I would do if I had more time." *Id.* at 31:10-17. Microsoft's expert, Prof. John Mitchell, agrees, identifying ten different variables (discussed below) that must be known to determine what is meant by "secure." Declaration of John Mitchell in Support of Microsoft's Motion Summary Judgment that Certain "Mini-*Markman*" Claims are Invalid for Indefiniteness ("Mitchell Decl.") at 8-11. Others involved in this industry, including some who have done, or do, business with InterTrust have testified to similar effect:

- MusicMatch; stated that in order to know whether a system is secure, one would have to know what the content provider for that system intended, and thus "security" as it applies to a particular system might mean something completely different from the same term applied to a different system. Ex. C, Jim McLaughlin Depo., p. 55:14-25.
- Envivio; stated that "secure" "doesn't mean anything in general. It means a general concept." Ex. D, Julien Signes Depo., at 40:22-41:2. When asked whether "it would be necessary ... to look at the context of the implementation of ... security to understand whether or not a system is secure," Mr. Signes answered, "yes, of course." *Id.* at 41:3-13.
- A leading authority in the field has written that "[w]ithout a precise definition of what security means and how a computer can behave, it is meaningless to ask whether a particular computer system is secure." Ex. E, Carl E. Landwehr, "Formal Models for Computer Security," ACM Computing Surveys, v.13 no. 3 (1981).
- "When someone states that 'My computer is secure,' that statement may very well mean distinctly different things to different people." Ex. F, Taylor, *Comparison Paper Between the Bell and LaPadula Model and the SRI Model*, IEEE Symp. on Security & Privacy, 1984, pg. 195, 197.

1. To Give "Secure" a Definite Meaning, a Number of Parameters Must Be Specified.

John Mitchell, a Professor of Computer Science at Stanford University, has identified ten parameters that persons of skill in the art would need to know in order to have a shared understanding of the meaning of "secure" in any given instance: (1) what types of things or actions are protected; (2) what specific things or actions are protected in the system in question; (3) what properties of those things are protected; (4) against whom; (5) against what points of attack; (6) against what kind of attack; (7) for how long; (8) to what degree of protection; (9) how is protection or the loss thereof evidenced; and (10) the perspective (or perspectives) from which "security" should be considered. Mitchell Decl., 8-11 and *passim*. To be able to evaluate whether an actual system is "secure," people of skill in the art must first reach a common understanding of each of these variables, as discussed below.

a. <u>What is to Be Protected</u>? (Mitchell Questions 1 and 2)

The first variable is, what is being protected? *See* Mitchell Decl., at 9. Is the user being protected from untrusted data, or is data being protected from untrusted users? *Id.* How "secure" is understood by people of skill in the art is influenced in the first instance by what one is trying to protect, and here the claims force them to guess. InterTrust has at least partly admitted that this is true. InterTrust objected to answering a Request for Admission that "a password-protected file is secure," on the ground that it was not told, *inter alia*, "the value of the information in the file." *See* Ex. G, InterTrust's Response to Microsoft Request for Admission 101. In InterTrust's view, in other words, the presence or absence of "security" depends on the nature of the thing to be protected. For a high-value item, a password requirement alone might not be enough to make the item "secure," while the same barrier might suffice to ensure the "security" of a low-value item.

b. <u>The Properties to be Protected</u>. (Mitchell Question 3)

The next crucial component of security is which attributes of the protected items are safeguarded. The different properties include:

- secrecy (or, "confidentiality") – maintaining the secrecy of data so that its meaning is not learned by unauthorized parties;
- integrity – ensuring that data may not be altered or destroyed by unauthorized parties;
- availability – ensuring that authorized parties can use the computers'

systems and data when desired;

- authenticity – ensuring accurate proof of the identity (or perhaps other characteristics) of the author or sender of a message or data;
- non-repudiation – preventing denial of the origination or receipt of messages by parties.

Mitchell Decl., 9-10. AOL and MusicMatch agree that security includes one or more of these components. AOL; Ex. H, Saccocio Depo., 30:8-31:16 (confidentiality, integrity, non-refutability, authentication); MusicMatch; Ex. C, McLaughlin Depo., 34:16-35:14 (integrity, authentication, non-repudiation, but not necessarily secrecy). So does InterTrust's expert, who testified that "secure" could be defined narrowly to include a single criterion, "secrecy," or in contrast, requiring satisfaction of the "Common Criteria," a multi-criteria framework for identifying security requirements and evaluating systems and whether they meet those requirements. Ex. A, Reiter Depo., 31:22-25, 32:15-20; Mitchell Decl., at 7, n. 1 (*see also* http://www.commoncriteria.org). Any one of these features alone, or any combination of them might suffice to create a "secure" system, depending on the context. The assurance of "availability" might be integral to the meaning of "secure" for one user, but not for another user with different priorities, as Dr. Reiter testified:

> Q: How about availability of information? Are you familiar with the concept of availability in...
>
> A. Sure, sure.
>
> Q. Are there some senses of the word secure where ensuring availability is required and other senses of the word secure where ensuring availability is not required?
>
> A. Yes, I'd say that's true.

Ex. A, Reiter Depo., 36:9-18 (objections and other non-substantive matter omitted).

c. <u>The Threats to be Protected Against (Against Whom, What Points of Attack, What Kind of Attack.)</u> (Mitchell Questions 4, 5, and 6)

Further crucial variables in defining "secure" are the types of attackers, the different possible points of attack, and the types of threats posed. Mitchell Decl., at 10. A system billed as "secure" against attack by outsiders might not be "secure" for a customer requiring a system that even insiders cannot misuse, or for a customer who requires protection not against its own employees but against a category of outsiders possessing certain identified information about the system or other special resources. *See, e.g.* Mitchell Decl., at 10, 20, 31, 34 (regarding "secure memory" "secure container," "secure operating environment" etc.).

The types of threats one has in mind are essential to defining "secure." As InterTrust itself argued in response to Microsoft Request for Admission that "a password-protected file is secure," one must know, *inter alia*, "the threats against which the file is to be protected." *See* Ex. G, InterTrust's Response to Microsoft Request for Admission 101. InterTrust's expert echoed this view, testifying that:

> "secure" is used as a general term to refer to protection against misuse and interference, **and to truly evaluate that security, you often need to be more precise about the sorts of misuse and interference you are concerned with, the threat models or the threats to which a system or primitive is likely to be subjected,** and the mechanism by which you protect that system.

Ex. A, Reiter Depo., 33:17-34:5 (emphasis added).

d. <u>The Duration and Degree of Protection</u>. (Mitchell Questions 7 and 8)

The duration and degree of protection are also prerequisites to understanding the meaning of "secure" in the art. Mitchell Decl., at 10-11. Withstanding an hour-long attack, or an attack employing a certain level of computing power might be sufficient in one context, but not another. Mitchell Decl., at 10. As to degree of protection, America Online's Director of Rich Media agreed that some notion of degree is needed to understand "secure":

> Q: But they [the criteria for "security"] can be met sufficient so that it's meaningful within this industry to use the term "secure," can they not?
>
> A: It's a vague term. I know it's frustrating, but it is. Security is a vague term. How much security is a better question.

Ex. H, Deposition of Damian Saccocio, 40:12-17.

///

///

e. How Protection is Verified and Evidenced. (Mitchell Question 9)

"Security" also depends on the manner in which continued protection, or the loss thereof, is or is not measured, tested, proven or evidenced analytically. Mitchell Decl., 11.

f. From Whose Perspective the System Is "Secure." (Mitchell Question 10)

Finally, the perspective from which "security" is viewed is crucial. A system can be "secure," or not, to a content owner, the system administrator, and or the authorized users. Mitchell Decl., at 11. Take for example, the case of a user who downloads a music file for a fee, which she pays electronically, using her credit card. If a third party tries to intercept the credit card information and make an additional, free copy of the downloaded file for himself, different outcomes could be viewed as "secure" by the different parties to the transaction. If the third party successfully copies the file, but not the credit card information, then the system might be considered "secure" from the perspective of the customer, but not the vendor. If, on the other hand, the attacker fails to copy the file, but does obtain the credit card information, and the system merely detects the unauthorized intrusion, then the vendor might consider the system "secure" while, from the customer's perspective, it is "insecure" – or at least the customer will see it that way, if she later learns of the theft.

B. The InterTrust Applicants Could Have Used the Claims or Specification to Adequately Define "Secure" But Failed to Do So.

1. InterTrust Has Not Defined "Secure" in the Claims or the Specification.

InterTrust could have chosen to define the term "secure" but didn't. Ten of the twelve claims at issue employ the word "secure" in some form, yet none of them defines it. Ex. J, JCCS Ex. H. They establish no security policy and no criteria that would answer the ten questions discussed above.

///

///

///

2. "Secure" Remains Indefinite Even When the Claim is Viewed in Light of the Specification.

Though "secure," and its variants, as used in the claims, lack requisite definiteness, the claims could still be saved from indefiniteness if "those skilled in the art would understand the scope of the claim when the claim is read in light of the rest of the specification." *Union Pac. Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684 (Fed. Cir. 2001). Far from curing the problem, however, the patent specification compounds it. It contains no uniform security policy, no uniform criteria for security, and no glossary. It uses "secure" and "security" in multiple, vague and inconsistent senses, giving the potential entrant into the field no more clarity than do the claims alone.

a) The Specification Describes Multiple Perspectives from which "Secure" Might Be Measured, and Indexes "Secure" to the Unpredictable Needs of Different Users

The specification uses "secure" in a fashion that is impossible for a person of skill in the art to understand because it depends on the unpredictable and varying needs of potential customers. In other words, "secure" cannot be defined completely by looking at the patent documents in light of the art. Instead, the '193 specification (Ex. Q) defines "secure" in terms of whatever the market may be seeking, which changes over time and has no fixed technological meaning:

- The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely. ('193 at 49:59-62)
- "a "sufficiently" secure (for the intended applications) environment" ('193 at 45:23-24)
- "with sufficient security (sufficiently trusted) for the intended commercial purposes" ('193 at 45:43-45)
- Development of such a standard has many obstacles, given the security requirements and related hardware and communications issues, widely differing environments, information types, types of information usage, business and/or data security goals, varieties of participants, and properties of delivered information. ('193 at 15:67-16:5).

b) The Specification Mentions Different and Inconsistent Secure Properties

The specification suggests several different security properties denoted by "secure" without committing to any of them. For example, "secure" could mean that an item or process is simply encrypted ('193 at 126:6-7), or "encrypted and tagged" (*id.* at 22:18-19), or "encrypted and authenticated" (*id* at 45:39-40), or not encrypted but "otherwise secured ... such as by employing authentication and/or error-correction" (*id.* at 63:37-39).

c) The Specification Mentions Many Different and Inconsistent Degrees of Security

The specification uses at least a dozen adjectives apparently identifying different "levels" of security – truly secure ('193 at 80:31, 81:14, 88:38); extremely secure ('193 at 67:21); highly secure ('193 at 22:16, 23:49, 36:9-10, 41:34, 67:19, 77:30, 104:63, 132:63, 203:66, 232:47, 233:4); commercially secure ('193 at 2:20, 47:6); adequately secure ('193 at 12:50); acceptably secure ('193 at 129:25); sufficiently secure ('193 at 9:12, 16:25, 21:48, 28:47, 49:41, 207:20, 249:51); appropriately secure ('193 at 77:16); physically secure ('193 at 13:20); sufficiently physically secure ('193 at 13:20); cryptographically secure ('193 at 202:44); continually secure ('193 at 32:4); relatively secure ('193 at 63:66); non-secure ('193 at 26:22, 49:10, 62:44, 73:56, 78:16, 77:43, 80:13, 80:20, 81:19, 120:38, 139:59, 229:20); possibly less secure ('193 at 80:33).

Though the meaning of these different degrees of security is unclear, it is evident that the degree of security, like the type of security, is a function of unpredictable factors in the marketplace outside the "world" of the patent. For instance, the patent claims that "[d]irect attack on these [cryptographic] algorithms is assumed to be beyond the capabilities of an attacker. For domestic versions of VDE 100 some of this is probably a safe assumption since the basic building blocks for control information have sufficiently long keys and are sufficiently proven." '193 at 221:12-17. But what was "sufficiently long" in 1995 may not be sufficiently long now or five years from now – that is a function of changes in the larger security environment. Elsewhere, the specification promises that "the VDE 100 provided by the preferred embodiment has sufficient security to help ensure that it cannot be compromised short of a successful 'brute force attack,' and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived." Ex. Q, '193 at 199:38-47. But the relationship between the cost of a "brute force attack" (essentially an attack that tries all possible keys no matter how long it takes) and the "value to be derived" by cracking a given system depends on the characteristics of the parties involved and changes in technology, which are "outside" the patent. The patent describes "secure" not in terms of technological means but in terms of ever-changing marketplace factors.

d) The Specification Mentions Different and Inconsistent Security Methods

Throughout the patent, different measures are desoribed as possibly sufficient for security, but no indication is given of which measures are necessary to security:

- "a secure enclosure, such as a tamper resistant metal container or some form of a chip pack containing multiple integrated circuit components" ('193 at 169:7-10)
- "In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information" ('193 at 59:55-58)

The attached declaration of Professor John Mitchell provides many more examples of the vague, multiple and inconsistent uses of "secure" and its variants in the patent specification. Mitchell Decl. at 12-17.

C. <u>The Prosecution History Does Not Give Secure a Clear Meaning</u>.

There is nothing in the prosecution history of any of the seven patents that resolves any of the problems discussed above. The prosecution histories do not offer any definition, criteria, or aid of any kind to help one of skill in the art understand what is meant by the term "secure" and its variants in the claims. Moreover, to the extent the continuation-in-part patents criticize the "big book" application as NOT teaching how to defend against a given threat (for example, "bogus load modules" that can "wreak havoc," (Ex. R, U.S. Patent No. 6,157,721 ("'721") '721 at 7:37, 8:16)), they raise even more questions about what "secure" could possibly mean in these claims.

D. Indefiniteness of Certain Patent Claims is Highlighted by Errors Made In The Specifications

1. The '683, '721 & '861 Patents Failed to Properly Incorporate the "Big Book" by Reference

An outside publication can be made part of a patent by referring to it, rather than actually reproducing its text. *See In re de Seversky*, 474 F.2d 671 (C.C.P.A. 1973). Whether material has been "incorporated by reference" is a question of law. *Advanced Display Systems, Inc. v. Kent State University*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). "Essential" material (*i.e.*, that which is necessary to describe the claimed invention) may only be incorporated by reference to an issued U.S. Patent or a published U.S. Patent Application. This requirement eases the burden on the public reviewing the patent, as it makes essential material readily available, whereas non-published material, like patent applications may not be available, or must be ordered at a considerable expense from the patent office. *See e.g.*, MPEP § 608.01 (p).

"The big book" material is "essential" in U.S. Patent No. 6,185,683 ("'683") (Ex. S) the '721, and U.S. Patent No. 5,920,861 ("'861") (Ex. V). In each of the patents, the "big book" is relied on to explain fundamental portions of the claimed inventions. *See* '721 at 4:51-60; '861 at 2:37-39; and '683 at 27:1-16.

2. None Of The Patents Met The "Incorporation By Reference" Requirements

The '683, '721, and '861 patents all purport to incorporate the "big book" by reference to the unpublished patent *application*. '721 at 1:7-19; '683 at 1:11-23; '861 at 1:7-11. They never amended their specifications to properly reference the issued patent number. This failure means that the "big book" materials are not part of the '721, '683 or '861 patents. Therefore, any need for definitions therefrom renders the claims and patents indefinite and invalid.

E. InterTrust Failed to Fulfill Its Obligation to Define the Claim Term "Secure" as Clearly as Possible.

The extrinsic evidence, including InterTrust's own documents, indicates that it had the opportunity to be more precise. In this regard, InterTrust not only failed to apprise what the bounds of the claim were, but also failed to be as precise as the subject matter permits. It is implicit in the lengthy discussion of parameters above that the term "secure" can be used with clear meaning in this field only after all the questions are answered. Typically this takes the form of a "security policy" and "criteria" for measuring satisfaction of that policy. A "security policy" answers "secure for whom?" and "secure for what purposes?" The security policy defines what is being protected against what attacks or threats (questions 1-6 of Mitchell Decl.). "Criteria" are designated as objective measurements for determining whether a real system satisfies the security policy. (Questions 7-10 of Mitchell). Together, the security polioy and criteria allow the word "secure," which otherwise is a general and merely conceptual term, to be used in a meaningful and definite manner. The InterTrust patent claims and specification contain no uniform security policy, and no uniform definition of "secure."

The need for a specific security policy and criteria is well known in the field:

> "A given system can only be said to be secure with respect to its enforcement of some specific policy." Ex. L, *Trusted Computer System Evaluation Criteria* (1985), pg. 59.
>
> *See also* Ex. M, Landwehr, Carl E. *How far can you trust a computer?*, SAFECOMP'93, Proc. of the 12th International Conf. on Compute Safety, Reliability, and Security, Poznan-Kiekrz, Poland, Oct., 1993, Janusz Gorski, ed., ISBN 0-387-19838-5, Springer-Verlag, New York, 1993.

As quoted above, InterTrust's expert, Dr. Reiter, affirmed the need to establish criteria to evaluate whether a real-world system is or is not, secure,[3] and recognized the role of a security policy in providing such criteria:

> [I]f a system has been evaluated via the common criteria, for example, to a given protection profile, this would be an example. You know, someone might say that it's secure once it's been evaluated via that framework. Ex. A, Reiter at 32:15-20.

F. <u>InterTrust's Proposed *Markman* Definition Confirms That "Secure" Is Indefinite.</u>

Although the claim construction stage of litigation is far too late to cure patent

[3] "'[S]ecure' is used as a general term to refer protection against misuse and interference, and to truly evaluate that security, you often need to be more precise about the sorts of misuse and interference you are concerned with, the threat models or the threats to which a system or primitive is likely to be subjected, and the mechanism by which you protect that system." Ex. A, Reiter at 33:23–34:5.

indefiniteness, it is telling that InterTrust did not even try to clarify the term. On the contrary, InterTrust's proposed definition of "secure" confirms its utter vagueness. InterTrust asserts that "secure" means that "[o]ne or more mechanisms are employed to ... disoourage misuse of or interference with information...," and can be achieved through "tamper resistance," elsewhere defined merely as "making tampering more difficult and/or allowing detection of tampering." Joint Claim Construction Statement filed in this Court on March 14, 2003. At the same time, InterTrust proposes that "[s]ecurity is not absolute, but is designed to be sufficient for a particular purpose." Joint Claim Construction Statement, at 6. Defining a claim relative to an unspecified "particular purpose" gives rise to precisely the uncertainty that Section 112(2) seeks to avoid. Moreover, whose perspective is sufficiency to be determined from and how are the "particular purposes" of the different users to be identified? By proposing a definition of "secure" that leads to inconsistent results, depending, for example, on who gets to specify a product's purpose, or whether its design is sufficient, InterTrust's own proposed definition confirms that the term has no definite meaning.

G. Nor Is "Secure" Redeemed By The Terms It Modifies.

None of the following claim phrases has a commonly shared understanding or usage in the field: "secure operating environment," "secure container," "secure memory," "secure database," "secure execution space," "securely applying," "securely assembling," "securely processing," or "securely receiving." Mitchell Decl., at 19-51. None of these terms resembles "smart card" or "hot dog," terms in which otherwise vague and subjective adjectives are made clear by that which they modify. In contrast, "secure" as it appears in the claims receives no assistance from the terms it modifies. A person of ordinary skill in the art would have to have answers to the questions discussed above to know in what sense each of these items is "secure." Intertrust's expert, Dr. Reiter, acknowledged that describing an item as "secure" does not, for instance, apprise one of whether it is protected against, say, denial of service attacks or attacks on causal logic, or whether the availability of information is ensured, to name just a few aspects of the concept. Ex. A, Reiter Depo., at 30-32; Mitchell Decl., at 6-7.

The problem with these compound terms is made intractable with InterTrust's argument that "secure" must have the same meaning everywhere it appears. In its *Markman* statement, InterTrust proposed defining "secure" independently for *Markman* purposes, and defining all other claim terms that incorporate it by reference to "secure". Thus, for "secure container," InterTrust proposes the definition, "a container that is Secure." *See e.g.*, JCCS, Ex. B. "Secure database," "secure execution space," "secure memory," and "secure operating environment" are all to be defined in analogous fashion. *Id.* Within InterTrust's proposed definitions of the phrases "securely applying," "securely assembling," "securely processing," and "securely receiving," the word "securely" is defined simply as "in a Secure manner." *Id.* InterTrust has bound itself to the position that all of these phrases must share a common definition of "secure." All claims containing that term, then, are indefinite and invalid.

H. INTERTRUST'S COINED TERMS "PROTECTED PROCESSING ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" ARE ALSO INDEFINITE.

In its patents, InterTrust introduces the terms "Protected Processing Environment" (or "PPE") and "Host Processing Environment" (or "HPE") — InterTrust coined these terms. Recognizing that they were new, proprietary terms, InterTrust often provides initial capitalization to the phrases or sets them off by quotation marks within the specification. (*See, e.g.* Ex.Q, '193 at 9:29, 13:10, 50:40, 105:18-19, 283:46)). These coined terms also appear in several claims including some of the mini-*Markman* claims (*e.g.* Ex. S, the '683 claim 2, and Ex. R, '721 claim 34.) It is the patentee's "duty to provide a precise definition" of terms unknown to those of ordinary skill in the art. *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F.3d 1563, 1570 (Fed. Cir. 1997).

1. THE TERMS "PROTECTED PROCESSING ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" HAVE NO ORDINARY COMPUTING ART MEANING.

The terms "Protected Processing Environment" ("PPE") and "Host Processing Environment" ("HPE") do not have an ordinary or customary meaning inside or outside of the computing world. They have not been found in any dictionaries that Microsoft has consulted. InterTrust has offered no dictionary or other extrinsic references to provide a meaning for these terms.

Significantly, even InterTrust's testifying expert confirmed that the terms would not have a known meaning to one of ordinary skill in the art in February 1995, when InterTrust submitted the "big book" application. Regarding the term "Protected Processing Environment," Dr. Reiter testified:

> Q. ...in February 1995, would the person of ordinary skill in the art have heard of the phrase protected processing environment?
>
> A. It's not a term in the art. One might assume certain things about that, but it's not a term in the Art.

(Ex. A, Reiter Depo., 131:22-132:2). He testified similarly that a person of ordinary skill would not be familiar with the term HPE. *Id.* at 132:3-6.

Not surprisingly, third party deponents, all of which had close dealings with InterTrust (most licensees of the asserted patents) were at a loss to assign any meaning, ordinary or otherwise, to these terms. *See* Ex. D, Envivio Depo. at 53:9-19 ("Q: Have you ever heard the term "protected processing environment"? A: No."); Ex. H, AOL Depo at 82:21-92:3; 96:4-97:17.

2. <u>THE CLAIMS DO NOT PROVIDE SUBSTANCE OR CONTEXT SUFFICIENT TO PROVIDE MEANING TO EITHER PPE OR HPE.</u>

These coined terms are used in three of the "Mini-*Markman*" claims: PPE is found in two and HPE is found in one. The claims do not provide the necessary context to formulate a sufficiently definite meaning.

The words of Claim 2 of the '193 patent, provide little information about what is meant by PPE. While it does partially indicate what is being protected, "*in part protecting information contained*", from what, "*from tampering*" and by who, "*by a user*", it still fails to inform one of ordinary skill if it "protects" "part" of the information or is "part" of the "protection". Also left open is what partial protection from tampering means. Does it merely detect that tampering has occurred, does it prevent tampering entirely or does it simply make tampering more difficult to achieve. It is impossible to divine from the claim language itself what is being claimed. As to its structure, the claim language recites merely that "said protected processing environment including hardware or software."

Other deficiencies can be seen in Claim 34 of the '721 patent. There, the open-ended identification of PPE as "comprising: a first tamper resistant barrier" which itself has a "first security level," a "first secure execution space," and "at least one arrangement" which prevents an identified operation. Conspicuously, this description relies on "secure" and "security." For the reasons noted above, this claim language lends no clarity to PPE but compounds its indefiniteness. Furthermore, one of ordinary skill cannot identify what is being "protected." *See* Mitchell Decl. at 35-37.

In Claim 155 of the '900 patent (Ex. T) InterTrust introduces another coined term "Host Processing Environment" (HPE). While Claim 155 attempts to provide an elaboration of what is meant by HPE through the use of the term "comprising," the description which followed only serves to obscure the meaning and scope of this new term.

While one of ordinary skill in the art reading Claim 155 could surmise that the HPE has at least a central processing unit, main memory and "mass storage," beyond this, the scope and reach of this term is indefinite. The claim goes on to assert that the "mass storage" of the HPE stores "tamper resistant software." This passage fails to set forth with meaningful clarity whether the tamper resistant software is an aspect of the Host Processing Environment. The base description of what *might* be parts of an HPE is insufficient to inform one of ordinary skill in this art as to what the meaningful boundaries and scope of this claim limitation are.

3. THE SPECIFICATION DOES NOT DEFINE THE TERM PROTECTED PROCESSING ENVIRONMENT.

Lacking a context or definition in the claims, the specification must be reviewed for guidance as to the term's meaning. The specification fails as well. InterTrust's first use of the term PPE in the '193 specification states merely that it is one component in a preferred embodiment of a VDE "secure subsystem." Ex. Q, '193 at 9:28. This provides neither information about, nor explanation of, what a PPE is or does. General reference is then made to the PPE in the "Brief Description of the Drawings" but no meaningful discussion, and certainly no definition is provided. '193 at 50:39-41. PPE is not again revisited until Col. 79, ln. 34. Here the patent states that a Host Event Processing Environment (HPE) 655 and Secure Event

Processing Environment (SPE) 503 "may be generically referred to as 'Protected Processing Environments' 650". In Column 105 (at ln. 17-22), the specification states simply that hereinafter in the specification, "unless context indicates otherwise, references to any of 'PPE 650,' 'HPE 655' and 'SPE 503' may refer to each of them." There is no substantive discussion of PPE after this entry.

InterTrust's treatment of PPE is fatally defective for multiple reasons. First, while being a coined term which refers to a feature central to InterTrust's VDE world (*i.e.*, "the invention"), it is never clearly described. At best, InterTrust attempts to give examples of what the "generic" usage of PPE <u>might</u> refer to. Both Secure Event Processing Environments (SPE) and Host Event Processing Environments (HPE) are "environments" which "may be generically referred to as 'Protected Processing Environments' 650". '193 at 79:30-35. In the first instance, InterTrust attempts to illuminate the meaning of a coined term with other coined terms, an unhelpful exercise. As InterTrust's expert identified, SPE and HPE are themselves terms which would not have been known to one of ordinary skill in the art in February 1995.

> Q. Okay. In February 1995, would the person of ordinary skill in the art have been familiar with the term host processing environment?
>
> A. I think not.
>
> Q. In February of 1995, would the person of ordinary skill in the art have been familiar with the phrase secure processing environment?
>
> A. So I have trouble putting my finger on specific usages of that of those three words that I would say were commonplace, but perhaps like protected processing environment, one might—who saw that might assume certain things, but—so I guess my answer would be no, it wasn't a well defined term in the field at the time, but put together they kind of make sense.

Ex. A, Reiter Depo., 134:6-16. Furthermore, there are marked differences between a HPE and SPE rendering the "generic class" to which PPE refers undefined. *See* Mitchell Decl. at 51-53.

To compound the confusion, in many instances where a feature or component of a PPE is set forth, it is qualified with the term "may" indicating that the described feature is optional, hence, may or may not be a part of PPE. This practice further obscures the inherently ambiguous nature of coined terms. For example, "Protected Processing Environment may refer generally to SPE and/or HPE . . ." (Ex. Q, '193 at 105:18-21). This invariably leaves the relevant public guessing at what might infringe. Such an unconstrained explanation fails to provide sufficient precision.

4. THE TERM HOST PROCESSING ENVIRONMENT IS NOT DEFINED IN THE SPECIFICATION EITHER.

The specification of the '900 patent (Ex. T) does not clear up what the claims leave vague. "Host processing environment" appears initially in the '900 specification in Col. 12 where it is identified that in "some embodiments" certain functions described in the specifications "may be performed by software, for example, in host processing environments of electronio appliances" Ex. T, '900 at 12:27-29 (emphasis added). This introductory use of the term "host processing environment" sheds no light on what it is, what it does or what its parameters are. The term is first used with all initial caps, indicating its coined nature, in Col. 3 at ln. 7, with no accompanying elaboration or definition. Aside from a passing reference in Col. 13, the term is not seen again until Col. 84, ln. 39 where it appears in the simple statement that "another instance of ROS [Rights Operating System] 602 might perform the same task using a *host processing environment* running in protected memory that is emulating a SPU in software." Again, this section of the specification does not elaborate on what the details or constituents of a "host processing environment" are.

As mentioned above with regards to "protected processing environment," the specifications suggest that "host processing environment," "protected processing environment" and "secure processing environment" are terms used as synonyms or as subsets of the other. The mingling of definitions of these coined phrases further aggravates the inherent ambiguity of their use in these patents.

III. ARGUMENT

A. Applicable Legal Standards

The patent statute requires that every patent include "one or more *claims particularly pointing out and distinctly claiming* the subject matter which the applicant regards as his invention." 35 U.S.C. § 112, ¶2 (emphasis added). Patent claims that fail to provide such fair warning are invalid. *Morton Int'l., Inc. v. Cardinal Chem. Co.*, 5 F.3d 1464, 1470 (Fed. Cir. 1993) (affirming holding of patent invalidity because "the claims at issue [were] not sufficiently precise to permit a potential competitor to determine whether or not he is infringing"). The Supreme Court explained the "definiteness" requirement and the "chilling" effect that indefinite patents have on legitimate competition as follows:

> The statutory requirement of particularity and distinctness in claims is met only when they clearly distinguish what is claimed from what went before in the art and clearly circumscribe what is foreclosed from future enterprise. A zone of uncertainty which enterprise and experimentation may enter only at the risk of infringement claims would discourage invention only a little less than unequivocal foreclosure of the field.

United Carbon Co. v. Binney & Smith Co., 317 U.S. 228, 236 (1942). Without abandoning that important principle, the Federal Circuit has made clear that "we have not held that a claim is indefinite merely because it poses a difficult issue of claim construction." *Exxon Research and Eng'g Co. v. United States*, 265 F.3d 1371, 1375 (Fed. Cir. 2001). Summarizing its requirements, the *Exxon* court stated:

> ... what we have asked is that the claims be amenable to construction, however difficult that task may be. If a claim is insolubly ambiguous, and no narrowing construction can properly be adopted, we have held the claim indefinite... By finding claims indefinite only if reasonable efforts at claim construction prove futile, we accord respect to the statutory presumption of patent validity (citation omitted) and we protect the inventive contribution of patentees, even when the drafting of their patents has been less than ideal.

Id. Indefiniteness must be shown by clear and convincing evidence. *L.A. Gear, Inc. v. Thom McAn Shoe Co.*, 988 F.2d 1117 (Fed. Cir. 1993). "The standard of indefiniteness is somewhat high; a claim is not indefinite merely because its scope is not ascertainable from the face of the claims." *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1342 (Fed. Cir. 2003). While the standard is high, "compliance with the written description requirement is essentially a fact-based inquiry that will "necessarily vary depending on the nature of the invention claimed." Quoting *Enzo Biochem v. Gen-Probe, Inc.*. 296 F.3d 1316, 1324 (Fed. Cir. 2002) (internal citation omitted). *Id.* at 1330 (affirming finding of indefiniteness). Further, "it is not [the court's] function to rewrite claims to preserve their validity." *Allen Eng'g Corp. v. Bartell Indus.*, 299 F.3d 1336, 1349 (Fed. Cir. 2002).

1. Claim Indefiniteness Requires a Two-Part Test

The test for determining whether a claim is definite is "whether those skilled in the art would understand the scope of the claim when the claim is read in light of the rest of the specification." *Union Pac. Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684 (Fed. Cir. 2001); *Morton*, 5 F.3d at 1470. The Federal Circuit has identified two parts to this test: 1) the patent claim, read in light of the rest of the patent and its Patent Office file, must "'reasonably apprise those skilled in the art'" as to its scope; and, 2) the patent claim must be "'as precise as the subject matter permits.'" *Amgen, Inc. v. Chugai Pharmaceutical Co.*, 927 F.2d 1200, 1217 (Fed. Cir. 1991), *quoting Shatterproof Glass Corp. v. Libbey-Owens Ford Co.*, 758 F.2d 613, 624 (Fed. Cir. 1985). InterTrust's patents fail both parts of the test, as demonstrated by both the intrinsic and extrinsic evidence.

2. "Secure" and Its Variants Are Indefinite Terms That Render the Claims Containing Them Invalid

The evidence is overwhelming that "secure" lacks a definite meaning in the art. It is a general term that both parties' experts and every third-party witness agree is vague unless given substantial context. InterTrust never provided the needed context in any part of its patents. Accordingly, persons of ordinary skill in the art cannot tell what "secure" means when reviewing the claims. "A claim term is indefinite if it can have more than one meaning to a person of ordinary skill in the art, and the appropriate meaning of the term is not explained in the specification" *See Union Pacific Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684, 692 (Fed. Cir. 2001) (finding the term "comparing" indefinite); *In re Cohn*, 58 C.C.P.A. 996, 438 F.2d 989, 993 (CCPA 1971) (finding claim term indefinite where the patentee's conflicting use of the term rendered the scope of the claims uncertain)." *VLT, Inc. v. Artesyn Techs. Inc.*, 238 F. Supp. 2d 339. Here, those of skill in the art, including InterTrust's own expert, have testified that secure can mean countless things to countless different people.

Although words of "degree" and other "relative" terms are sometimes upheld, "when a word of degree is used, the district court must determine whether the patent's specification provides some standard for measuring that degree." *See Seattle Box Company, Inc., v. Industrial Crating & Packaging, Inc.*, 731 F.2d 818, 826 (Fed. Cir. 1984). Here, as shown above, the speoification not only fails to provide the necessary context, it adds to the ambiguity. Without some constraining parameters, subjective adjectives like "secure" are indefinite. A predecessor to the Federal Circuit, for example, affirmed the rejection of claims using the "relative" terms "stiff" and "resilient" (describing brush bristles) because the patent provided no guidance as to how stiff or how resilient. *See Application of Lechene*, 277 F.2d 173, 176 (C.C.P.A. 1960). Stiff, unlike "secure," is one-dimensional – the only question was "how stiff?" "Secure" raises not only the question of "how secure," but also, "what kind of security," "from whom," and so on.

Moreover, InterTrust's indexing of "secure" to customer preferences in the specification makes it comparable to a rejected claim brought before the Board of Patent Appeals and Interferences in *Ex parte Brummer*, 12 USPQ2d (BNA) 1653 (BPAI 1989). In *Brummer*, the claim was directed to an improved recumbent bicycle having "a wheelbase that is between 58 percent and 75 percent of the height of the rider that the bicycle was designed for." The Board held that "whether the bicycle was covered by the claim would be determined not on the basis of the structural elements and their interrelationships, as set forth in the claim, but by means of a label placed upon the bicycle at the discretion of the manufacturer." *Id* at **3-4. The Board noted that with such claim language, a claim may be infringed when ridden by one rider, but not when ridden by another. Similarly, because the "level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely," (Ex. Q, '193 at 49:59-62), the scope of the claims depends on unpredictable, ill defined and ever-changing market factors. Indeed, InterTrust's use of "secure" is more indefinite than the language at issue in *Brummer*. In that case, the indefinite language allowed the patentee to vary the meaning of the claims as to one variable (size of the wheelbase); InterTrust's claims apparently seek leeway to shift and remold themselves along all of the different axes of "security" discussed above.

Finally, secure and its variants further fail the definiteness requirement in failing to be as "precise as the subject matter allows." As demonstrated by its own documentation and by the widespread availability of model security policies, InterTrust had the ability to provide more definite meanings. It did not, and therefore the claim terms are not "as precise as the subject matter permits." *Amgen, Inc. v. Chugai Pharmacetical Co.*, 927 F.2d 1200 at 1217.

Claim indefiniteness is particularly problematic where it derives from "conveniently functional language at the exact point of novelty." *General Electric Co. v. Wabash Appliance Corp.*, 304 U.S. 364, 371-372, 58 S. Ct. 899, 902-03 (1938). As InterTrust's own expert testified, "security" is an "essential aspect" of the alleged invention. Reiter Depo., at 23:21-24:9. Accordingly, although no term should be ambiguous in a patent claim, it is particularly inexcusable that this "core" term be left hopelessly vague. *Exxon Research & Engineering Co. v. United States*, 265 F.3d 1371, 1379 (Fed. Cir. 2001) (fatal for limitations critical to patentability to be indefinite).

B. <u>New Or Coined Terms Must Be Defined Or Otherwise Made Clear.</u>

If the patentee elects to use "a term with no previous meaning to those of ordinary skill in the art ... [i]ts meaning ... must be found somewhere in the patent." *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F.3d 1563, 1568 (Fed. Cir. 1997) (emphasis added). In introducing the coined terms "protected processing environment" and 'host processing environment," InterTrust had a "duty to provide a precise definition" for them. It failed to do so. Accordingly, these terms are indefinite and the claims containing them, invalid.

///

///

///

///

///

///

///

IV. CONCLUSION

For the foregoing reasons, and those set forth in the accompanying Report and Declaration of Professor Mitchell, the Court should grant partial summary judgment that the following eleven claims are indefinite and invalid under 35 U.S.C. § 112, ¶ 2: claims 1, 11, and 15 of the '193 patent; claim 2 of the U.S. Patent No. 6, 185,683; claims 1 and 34 of U.S. Patent No. 6,157,721; claim 58 of U.S. Patent No. 5, 920,861; claim 1 of U.S. Patent No. 5, 982,891; claim 155 of U.S. Patent No. 5,892,900; and claims 8 and 35 of U.S. Patent No. 5,917,912.

Dated: March 17, 2003

WILLIAM L. ANTHONY
ERIC L. WESENBERG
KENNETH J. HALPERN
ORRICK, HERRINGTON & SUTCLIFFE LLP

Eric L. Wesenberg
Attorneys for Defendant and Counterclaimant
MICROSOFT CORPORATION

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

DERWIN & SIEGEL, LLP
DOUGLAS K. DERWIN - #111407
3280 Alpine Road
Portola Valley, CA 94028
Telephone: (408) 855-8700
Facsimile: (408) 529-8799

INTERTRUST TECHNOLOGIES CORPORATION
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

AND COUNTER ACTION.

Case No. C 01-1640 SBA (MEJ)

Consolidated with C 02-0647 SBA

MEMORANDUM OF POINTS AND AUTHORITIES OF PLAINTIFF INTERTRUST TECHNOLOGIES IN OPPOSITION TO MICROSOFT MOTION FOR SUMMARY JUDGMENT ON INDEFINITENESS AND IN SUPPORT OF CROSS-MOTION FOR SUMMARY JUDGMENT

Date: May 30, 2003

TABLE OF CONTENTS

TABLE OF CONTENTS
(cont'd)

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES
(cont'd)

Statutes

I. INTRODUCTION

The word "secure" is widely used in the computer security field. It appears in the claims of hundreds of patents, including many issued to Microsoft. It is used in product documentation, technical literature and white papers published by Microsoft and others. It is defined in numerous technical dictionaries, including the Microsoft Computer Dictionary.

Yet Microsoft now seeks to convince the Court that the word "secure," when used in InterTrust patent claims, is so vague that it renders those claims indefinite as a matter of law.

InterTrust's patents are presumed valid, and Microsoft carries a heavy burden of establishing, by clear and convincing evidence, that one of ordinary skill in the art would be unable to understand or apply the claims. This burden is considerably heavier where, as here, the disputed term is widely used by the defendant, by others in the field, and in numerous patents.

Microsoft cannot possibly carry its burden. It relies on a test manufactured by its expert witness, Professor Mitchell, for the purpose of this litigation, a test never applied to any other document, a test that is so stringent that it is failed by Microsoft patents, third party patents and industry documents. In fact, Professor Mitchell's published papers fail his own test! There is no evidence that any document ever created anywhere, by anyone, can pass Prof. Mitchell's test.

InterTrust's patents use the term "secure" in a manner consistent with the generally understood use of that term in the industry. Microsoft uses the term in exactly the same manner in its own patents and documents. Microsoft cannot carry its burden. InterTrust therefore seeks summary judgment that the disputed claims are definite.

II. FACTS

A. "Secure" and "Security" Are Widely Used in the Computer Security Field.

The terms "secure" and "security" are widely used in the computer security field to refer to the application of one or more mechanisms to protect a computer system or process against attack. Mitchell Decl., 4:18-19; Reiter SJ Decl., ¶¶ 5-7.[1]

[1] Declaration of Dr. Michael Reiter in Opposition to Microsoft Motion for Summary Judgment on Invalidity and In Support of InterTrust's Cross-Motion.

1. General use in the industry.

a. Dictionary definitions. "Secure" and "security" are defined in many computer dictionaries. Those definitions use different language, but consistently focus on protection against a type of attack or misuse. Reiter SJ Decl., ¶ 7(a); McDow Decl., ¶ 5 and Ex. C.[2]

b. Microsoft and third party documentation. Microsoft routinely uses the words "secure" and "security" to refer to its own products. Reiter SJ Decl., ¶¶ 14-22, 27. For example, Microsoft describes how its Windows operating system was evaluated under a standard security methodology, including statements such as "Windows 2000 meets the evaluation requirements by providing secure directory access and administration." This document also describes features such as "secure connectivity," "secure policy application," and "secure networked environment." Reiter SJ Decl., ¶ 16 and Ex. J. This use of "secure" to describe products or product features is common in Microsoft documents. Reiter SJ Decl., ¶ 27 and Ex. C, Page Decl., Ex. C.

Dr. Reiter analyzed publicly-available Microsoft technical documents that use the term "secure." They do not pass Prof. Mitchell's test. Reiter SJ Decl., ¶ 27 and Ex. C.

Microsoft's use of "secure" to refer to its products and features is not limited to public documents. In internal documents, Microsoft engineers describe products as "secure," with no apparent difficulty in understanding what the term means. These include terms that are identical or extremely similar to the terms Prof. Mitchell has decided are "unclear." Derwin Decl.,¶¶ 3-6.[3]

"Secure" is also routinely used in third party documents without definition. Reiter SJ Decl., ¶7(b) and Ex. L, Page Decl., Ex. B.

2. Use in Prof. Mitchell's papers.

Prof. Mitchell's papers use the term "secure" or "securely." Dr. Reiter applied Prof. Mitchell's test to these papers. The papers do not pass the test. Reiter SJ Decl., ¶ 26 and Ex. F.

[2] Declaration of Jeff McDow in Opposition to Microsoft Motion for Summary Judgment on Invalidity and In Support of InterTrust's Cross-Motion.

[3] Declaration of Douglas Derwin In Opposition to Microsoft Motion for Summary Judgment and In Support of InterTrust's Cross-Motion.

3. Use in other patents.

a. Microsoft patents. The term "secure" is used as an adjective or adverb describing computer products or processes in the claims of numerous Microsoft patents, including one of the patents Microsoft has asserted against InterTrust in a counterclaim in this action. McDow Decl., ¶ 6 and Ex. D; Reiter SJ Decl., ¶¶ 7(c), 28 and Ex. D.

Microsoft's patents include claims with terms such as: "secure mode," "securely stores," "secure function," "securely shared," "secure access," "secure network," "secure data," "securely integrated," "secure message" and "secure package." McDow Decl., Ex. D.

Dr. Reiter analyzed a number of the Microsoft patents. None of them passes Prof. Mitchell's test. Indeed, the Microsoft patents contain less information about what "secure" means than do the InterTrust patents. Reiter SJ Decl., ¶ 29.

b. Third party patents. Ex. E to the McDow Decl. illustrates the use of "secure" in the claims of 100 computer-related patents issued over the past year, including phrases such as "secure element," "secure server," secure environment" "secure Internet access," "secure storage device," secure data" and "secure operating system." Dr. Reiter checked several of these patents, none of which can pass Prof. Mitchell's test. None of them includes as much information about what "secure" means as do the InterTrust patents. Reiter SJ Decl., ¶¶ 30-31.

B. Recognized Methodologies Exist for Determining if Computer Products or Methods are Secure.

Dr. Reiter describes several recognized methodologies for determining if computer products are "secure," some of which are explicitly referenced in the InterTrust patents. Reiter SJ Decl., ¶¶ 13-23. Computer security professionals routinely use such methodologies to determine if products or methods are "secure," and purchasers (including the U.S. Government) routinely rely on these determinations in making purchasing decisions. Reiter SJ Decl., ¶ 13.

Dr. Reiter's Declaration includes a description of a Microsoft marketing document explaining how one such methodology was applied to Microsoft Windows, and declaring that elements of the product had been found to be "secure." Reiter SJ Decl., ¶¶ 14-22 and Ex. J.

The information included in the InterTrust patents includes guidance regarding how security should be measured, including the statement that security should be based on a commercially reasonable standard.[4] Computer security professionals routinely apply such a standard in building security into real-world products. Reiter SJ Decl., ¶¶ 12, 18.

C. The Experts Agree on the General Meaning of "Secure" and "Security."

InterTrust and Microsoft have each proposed a definition for "secure." Those definitions are generally consistent, the primary difference being Microsoft's insistence that each of five specific properties be protected, whereas InterTrust's definition is: "One or more mechanisms are employed to prevent, detect, or discourage misuse of or interference with information or processes." This definition is definite, it is easily understood and simply applied, and provides clear guideposts for determining whether a specific system falls within its scope.

Microsoft's expert, Professor Mitchell and InterTrust's expert, Dr. Reiter, agree that "secure" and "security" have a general meaning in the field. Reiter SJ Decl., ¶ 5. In his Declaration, Prof. Mitchell explains this general meaning:

> In computer science, including the particular fields most pertinent to these InterTrust patents, "security" generally has to do with designs, techniques and mechanisms for protecting certain properties against some kinds of attack or adversarial conditions.

Declaration of Professor John C. Mitchell ("Mitchell Decl."), 4:15-17. Prof. Mitchell's deposition testimony, quoted at McDow Decl., Ex. A, § 1, is consistent with this understanding:

> A. Well, security generally has to do with guaranteeing certain properties against some kind of attack or adversarial conditions.

Mitchell I, 29:6-8.[5]

> We use the word "secure" to suggest that there are some properties being protected against an adversarial attack.

Mitchell I, 88:5-7.

> I mean, ordinarily, and almost uniformly, "security" is a term that suggests one or more properties against one or more threats where the properties and threats are determined by the context in which you use it.

[4] See, e.g., items 19(B) and 19(J) from Joint Claim Construction Statement, Ex. C, which contains InterTrust's evidence in support of its claim construction position.

[5] In transcript quotations, extraneous material (e.g., objections) is omitted.

Mitchell I, 117:8-12.

Professor Mitchell also testified that those of ordinary skill in the art can determine if a product is "secure" through commonly used methodologies or criteria. That testimony, which is quoted in McDow Decl., Ex. A, § 2, includes the following:

> Q. Is it ever possible to determine if a system is secure, in your opinion?
>
> A. There are compelling arguments that can be presented to substantiate a claim of security. There's a recognized set of criteria, or several proposed sets of criteria, for establishing or certifying security systems.

Mitchell I, 46:20-47:1.

> Q. So I take it that there are a range of methods that a security analyst might use to determine if a system is secure, correct?
>
> THE WITNESS: Yes. A security analyst, given a set of properties and a set of possible attacks or looking for attacks, could use a number of different methods to study a system.
>
> Q. Was that also true as of February 1995?
>
> A. I believe so.

Mitchell I, 53:11-21.

Prof. Mitchell's testimony on this issue is clear, consistent and unambiguous:

(a) "Secure" means that properties of a system are protected against attacks.

(b) To determine if a particular system is "secure," it is necessary to perform an investigation to determine what the protected properties are, what the potential attacks are, and whether the former are protected against the latter.

(c) There are recognized methodologies used to perform this investigation.

D. The InterTrust Patents Use the Terms "Secure" and "Security" Consistently with the Generally Accepted Meaning of these Terms.

Prof. Mitchell understands what "secure" means in the patents. His testimony is quoted at McDow Decl., Ex. A, § 3. Following are some of the highlights:

> A. I don't find any place in the patent where it says, "In this document, 'secure' means the following." So in that sense, I don't really see a definition of "security" here.
>
> However, the patent describes or suggests or promises a set of properties, and

they include these five properties, as I understand it.

Q. Okay. And these five properties are the properties availability, secrecy, integrity, authenticity, and nonrepudiation that are listed in the Microsoft construction for "secure," correct?

A. I believe that's what we're discussing, yes.

Mitchell I 68:25-69:11.

Were you able in some cases to determine what the patent meant by the use of the word "secure"?

A. I'm having a little trouble putting my finger on or imagining a specific case to give you as an example. But there are some passages where there are descriptions of -- that are a little more specific and give some reasonable guess as to which of these properties are relevant in that situation.

Q. Are there some passages in the '193 patent in which the word "secure" is used to refer to a subset of these five properties?

THE WITNESS: Yeah. I mean, it may be in the sense I just described.

Mitchell I, 74:20-75:10.

Microsoft's argument that "secure" is used inconsistently in the InterTrust patents is based on a mischaracterization of the patents. Thus, Microsoft points out that the InterTrust patents use a variety of adjectives to modify "secure, and argues that "the meaning of these different degrees of security is unclear." MS Memo. at 10:20. The passages cited by Microsoft, however, explicitly explain the differences between many of these terms. Thus, "truly secure" and "less secure" occur in the same sentence, with the former characterizing processing using a Secure Processing Unit whereas the latter characterizes processing using a Host Processing Environment. '193 Patent, 80:22-35. These terms are not used in isolation, but are explicitly explained and contrasted. Similarly, the '193 patent contains a passage contrasting "highly secure" encryption algorithms with "extremely secure" algorithms, and explicitly identifies each type of algorithm, including explaining circumstances under which each should be used. '193 Patent, 67:18-40. See also '193 Patent, 201:63-202:12. Again, these uses are not evidence that "secure" is meaningless, but instead include significant clarifying detail, detail that Microsoft and Prof. Mitchell ignore. Each of these passages uses the term "secure," and each of them serves as an example of the meaning of the term "secure" in the claims (e.g., both "highly secure" and "extremely secure" algorithms are "secure.")

Prof. Mitchell understands what "secure" means in the InterTrust patents: in general it means protection of the five listed properties, but sometimes the word refers to protection of fewer than all five. This testimony is consistent with InterTrust's proposed definition of "secure" and with Dr. Reiter's testimony. Reiter SJ Decl., ¶¶ 5 and 7(d).

E. Prof. Mitchell's Declaration Establishes that the Disputed Terms Are Definite and Clear.

Prof. Mitchell understands the meaning of the disputed terms. The first claim term analyzed in his Declaration is "secure memory." He first explains what the term means:

> Thus, the "secure memory" must at least be able to store a file whose copying or moving is prevented, except as authorized.

Mitchell Decl., 20:10-18.

Prof. Mitchell thus understands that a "secure memory" must prevent unauthorized copying or moving of a file.

Prof. Mitchell next discusses use of "secure memory" in the art (Mitchell Decl., 20:20-25), then turns to descriptions of the term in the patent specification. He quotes over 30 lines of detailed description from a specification embodiment of "secure memory," including protection mechanisms and the actions prevented (e.g., information cannot be observed, interfered with or leave except under appropriate conditions).

InterTrust may not agree with Prof. Mitchell's construction of "secure memory" when that phrase is presented for construction. Nevertheless, the fact that Prof. Mitchell is able to articulate a clear definition of the term demonstrates that "secure" is not indefinite.

The next term analyzed by Prof. Mitchell is "secure container." Again, he analyzes the term, extrinsic evidence and the specification and concludes as follows:

> This method [861.58] appears to promise that it prevents anyone and anything from accessing or using certain information (by putting the information in a secure container), except as authorized by a rule. (Mitchell Decl., 26:3-6)
>
> The component assembly [in 912.35] is protected in at least three ways: (a) one of its elements is shielded from unauthorized access (by a secure container), (b) the record identifying the elements necessary to build the component assembly is

> likewise protected . . . .(Id., 26:22-26)
>
> This language from '683, Claim 2 . . . suggests that the 'secure container' is able to prevent 'an aspect of access to or use of' its governed items . . . .(Id., 27:22-25)

Thus, Prof. Mitchell understands "secure container" similarly in all three claims: the container shields or protects its contents from access or use.

Similar points can be made about Prof. Mitchell's discussion of the other purportedly indefinite claim terms: in each case his Declaration reveals he understands what the term means.

Prof. Mitchell's opinion that "secure" is indefinite is not based on any failure to understand the claim terms, but instead on InterTrust's failure to meet a ten-part test that takes up two pages in his Declaration. Mitchell Decl., 9:3-11:4. However, Prof. Mitchell admitted in his deposition that he had created this test for purposes of this litigation, after deciding that more standard methodologies were too "technical" for the Court to understand. Mitchell II, 223:13-16. McDow Decl., Ex. A, § 5, Reiter SJ Decl., ¶¶ 2, 24. Tellingly, Prof. Mitchell made no attempt to apply his test to any other document. See Mitchell testimony in McDow Decl., Ex. A, § 6.

Not surprisingly, when Prof. Mitchell's test is applied in other contexts, it turns out that Microsoft's security-related technical documentation also fails his test, Microsoft's patents fail his test, third party patents fail his test, and <u>Prof. Mitchell's own computer security papers</u> fail his test. Reiter SJ Decl., ¶¶ 25-32 and Exs. C-F.

Moreover, Prof. Mitchell's application of this test is revealing. For example, he does not feel that InterTrust's "secure memory" meets test item (2), since "There is no indication, e.g., of what information in addition to the file is to be stored." Mitchell Decl., 23:8-9.

The relevant claim (193.1) states that the secure memory contains a digital file. It does not require any other information, and Prof. Mitchell does not argue that the claim includes any such requirement. Mitchell II, 292:17-293:17. Thus, InterTrust fails his test because the claim does not identify other information the presence of which is not required by the claim.

Similarly, Prof. Mitchell testifies that item (3) from his test hasn't been met since "There is no clear indication of whether the stored information's availability, integrity or authenticity is to be protected." Mitchell Decl., 23:10-11. Earlier in the Declaration, however, he noted that the claim requires that copying or moving the file be prevented, except as authorized. Mitchell Decl., 19:10-11. Similarly, he understands specification references to "secure memory" to mean that "a 'secure memory' is 'secure' in part because all unauthorized access to, observation of, and interference with information stored within it is prevented." Mitchell Decl., 21:11-14.

Thus, according to Prof. Mitchell, the claim and the specification embodiment clearly explain what is being protected.[6] Prof. Mitchell does not explain why it is necessary for the claim to also list other elements the protection of which is not required by the claim.

To take one last example, Prof. Mitchell finds "secure operating environment" indefinite despite the following: "The patents suggest that a 'secure operating environment' is 'secure' in part because it prevents all unauthorized access to, and observation of, and interference with data and processes within the operating environment." Mitchell Decl., 33:7-9. Despite this, Prof. Mitchell nevertheless finds the term indefinite because it doesn't pass his test.

Prof. Mitchell understands the claim terms, but argues they are unclear because they do not include enough information to pass his made-up ten-part test, including information that is clearly extraneous to the claim. The Federal Circuit has a name for analysis of this type: semantic quibbling. Rosemount, Inc. v. Beckman Instruments, Inc., 727 F.2d 1540, 1548 (Fed. Cir. 1984).[7] Microsoft cites no legal support for the proposition that a claim may be invalidated for indefiniteness based on its failure to recite extraneous details. No such support exists.

F. The InterTrust Patents Contain Significant Information About Every Element of Prof. Mitchell's Test.

Even if Prof. Mitchell's test were accepted in the industry, InterTrust's patents contain a

[6] InterTrust does not necessarily agree with Prof. Mitchell's interpretation of "secure memory" or other terms he discusses. Those terms may have to be construed by the Court in subsequent proceedings, and InterTrust will present its position on their meaning at that time. The significance of Prof. Mitchell's testimony is not that he agrees with InterTrust's interpretation of the claims, but that he has no difficulty coming to an interpretation, thereby clearly indicating that the claims are not indefinite. That parties disagree about the meaning of the claims does not render them indefinite. See below, § III B 3.

[7] "Beckman attacks the claims as indefinite, primarily because 'close proximity' is not specifically or precisely defined. . . . [T]o accept Beckman's contention would turn the construction of a patent into a mere semantic quibble that serves no useful purpose."

wealth of detail responsive to every element of that test, detail that Prof. Mitchell ignores. Reiter SJ Decl., ¶ 38 and Ex. B, § II. Prof. Mitchell's ignorance of key passages is understandable, since InterTrust identified specification passages of greatest significance to the disputed terms, but Microsoft failed to provide this information to him. McDow Decl.,¶¶ 9-10 and Ex. A, § 8. These passages provide significant detail on the terms, including very important elements not described in the passages quoted in Prof. Mitchell's Declaration. Reiter SJ Decl., ¶¶ 44-48.

III. ARGUMENT

A. Microsoft Carries a Heavy Burden of Establishing Indefiniteness By Clear and Convincing Evidence.

InterTrust's patents carry a "strong presumption of validity," and the burden is on Microsoft to rebut that presumption with "clear and convincing evidence." Al-Site Corp. v. VSI Int'l, Inc., 174 F.3d 1308, 1323 (Fed. Cir. 1999); Intel Corp. v. Via Techs., Inc., 319 F.3d 1357, 1366 (Fed. Cir. 2003) ("Any fact critical to a holding on indefiniteness, moreover, must be proven by the challenger by clear and convincing evidence"). In ruling on Microsoft's indefiniteness defense, the Court must resolve close questions in favor of InterTrust. Exxon Research & Eng'g Co. v. United States, 265 F.3d 1371, 1380 (Fed. Cir. 2001).

B. Indefiniteness Standards.

In Exxon Research, the Federal Circuit provided an overview of the indefiniteness analysis, emphasizing the difficult burden facing a party seeking to establish that the claims of an issued U.S. Patent are invalid for indefiniteness:

> In determining whether that standard is met, i.e., whether "the claims at issue [are] sufficiently precise to permit a potential competitor to determine whether or not he is infringing," we have not held that a claim is indefinite merely because it poses a difficult issue of claim construction. We engage in claim construction every day, and cases frequently present close questions of claim construction on which expert witnesses, trial courts, and even the judges of this court may disagree. Under a broad concept of indefiniteness, all but the clearest claim construction issues could be regarded as giving rise to invalidating indefiniteness in the claims at issue. But we have not adopted that approach to the law of indefiniteness. We have not insisted that claims be plain on their face in order to avoid condemnation for indefiniteness; rather, what we have asked is that the claims be amenable to construction, however difficult that task may be. If a claim is insolubly ambiguous, and no narrowing construction can properly be adopted, we have held the claim indefinite. If the meaning of the claim is discernible, even

> though the task may be formidable and the conclusion may be one over which reasonable persons will disagree, we have held the claim sufficiently clear to avoid invalidity on indefiniteness grounds. By finding claims indefinite only if reasonable efforts at claim construction prove futile, we accord respect to the statutory presumption of patent validity and we protect the inventive contribution of patentees, even when the drafting of their patents has been less than ideal.

Exxon Research, 265 F.3d at 1375 (citations omitted).

1. Whether one of ordinary skill in the art would understand the claim.

To carry its burden, Microsoft must establish that one of ordinary skill in the art would not be able to understand the scope of the claims, read in light of the specification. North Am. Vaccine v. American Cyanamid Co., 7 F.3d 1571, 1579 (Fed. Cir. 1993). In making this determination, the Court must keep in mind that patents are not required to include information that would be understood by one of ordinary skill:

> Patent documents are written for persons familiar with the relevant field; the patentee is not required to include in the specification information readily understood by practitioners, lest every patent be required to be written as a comprehensive tutorial and treatise for the generalist, instead of a concise statement for persons in the field. Thus resolution of any ambiguity arising from the claims and specification may be aided by extrinsic evidence of usage and meaning of a term in the context of the invention. The question is not whether the word "substantially" has a fixed meaning as applied to "constant wall thickness," but how the phrase would be understood by persons experienced in this field of mechanics, upon reading the patent documents.

Verve, LLC v. Crane Cams, Inc., 311 F.3d 1116, 1119-20 (Fed. Cir. 2002).

2. Use of general terms to describe a range of circumstances does not render claims indefinite.

Claims may use general terms to describe a range of circumstances, as long as those of ordinary skill in the art would be able to understand the terms. In Exxon Research, the Federal Circuit found a claim term not indefinite despite the fact that the presence of the claim element would depend on external factors, including the conditions chosen for the claimed process:

> Although the patent does not quantify the "period sufficient" limitation by reference to any specific period or range of periods, it does not leave those skilled in the art entirely without guidance as to the scope of that requirement. . . .
>
> * * *
>
> Because the patent makes clear that the period in question will vary with changes in the catalyst and the conditions in which the process is run, we conclude that the claim limitation is expressed in terms that are reasonably precise in light of the

subject matter.

Exxon Research , 265 F.3d at 1379.

Similarly, in Orthokinetics, Inc. v. Safety Travel Chairs, Inc., 806 F.2d 1565, 1576 (Fed. Cir. 1986), the Federal Circuit held that a claim term was not indefinite despite the use of general language the application of which would necessarily depend on the circumstances:

> [Claim] 1. In a wheel chair having a seat portion, a front leg portion, and a rear wheel assembly, the improvement wherein said front leg portion is so dimensioned as to be insertable through the space between the doorframe of an automobile and one of the seats thereof . . . .
>
> * * *
>
> The claims were intended to cover the use of the invention with various types of automobiles. That a particular chair on which the claims read may fit within some automobiles and not others is of no moment. The phrase "so dimensioned" is as accurate as the subject matter permits, automobiles being of various sizes. _As long as those of ordinary skill in the art realized that the dimensions could be easily obtained, § 112, 2d para. requires nothing more. The patent law does not require that all possible lengths corresponding to the spaces in hundreds of different automobiles be listed in the patent, let alone that they be listed in the claims.

Orthokinetics, 806 F.2d at 1576 (citation omitted).

Thus, in Orthokinetics the Federal Circuit held "so dimensioned" to be sufficiently definite, despite the fact that a chair "so dimensioned" as to fit into one car would not necessarily fit into another car. The Federal Circuit held that it was unnecessary for the patentee to list all of the possible dimensions in the claim, or in the body of the patent itself. This ruling is in direct contrast to Microsoft's methodology.

The district courts have held similarly, rejecting indefiniteness arguments based on claim elements the presence of which depends on external circumstances:

> As with selectivity, whether an antibody has a useful degree of affinity appears to depend on several factors. Genentech's expert, Dr. Unkeless, testified at his deposition that the affinity value required for an antibody to work for purposes of diagnosis may vary depending on the type of assay that is used.
>
> * * *
>
> . . . If, as Dr. Unkeless suggests, it is impossible to define a useful level of affinity by reference to a particular numerical value, the '561 patent cannot be expected - and is not required as a matter of law - to list every possible affinity value that might be useful for every possible purpose of the invention.

> Moreover, simply because a broad range of affinities may be useful does not make the claims indefinite. It is well settled that breadth is not to be equated with indefiniteness." . . . Thus, the claims may permissibly encompass a wide range of affinity values . . . . The relevant question is whether a person of ordinary skill in the art would understand when a monoclonal antibody has an affinity value that is "useful" for the purposes described in the specification.

Chiron Corp. v. Genentech, Inc., No. Civ. S-00-1252, 2002 U.S. Dist. LEXIS 19150, *10-11 (E.D. Cal. June 24, 2002) (citations omitted).[8]

> The Court . . . finds that the term "substantial" as used in the context of paving installations described in the '550 Reissue Patent is sufficiently precise to inform one skilled in the art. . . . in the context of paving installations like those described in the '550 Reissue Patent which can be subjected to a wide variety of loads, it is understood that no explicit quantification can be made for such forces. Thus, the term "substantial" cannot be interpreted to mean a specific quantity; rather it describes a range of loads from pedestrian to vehicular to occasional heavy truck. Dr. Witczak further testified that while tractor-trailers and commercial aircraft would certainly produce "substantial" forces, it is understood from the patent that this invention would not be applied in installation subject to such forces. . . .
>
> * * *
>
> The Court finds that the term "substantial," when considered in the light of the entire claimed invention, is as accurate as the subject matter permits and provides sufficient guidance to one skilled in the art of paving stone installations. . . . Given that pedestrians and vehicles come in a myriad of shapes and sizes, it would be impossible to set forth every possible specific force. Thus, the use of the term "substantial forces" adequately explains that walkways and driveways which incorporate this interlocking paving installation can be subjected to a limited range of forces - from pedestrians up to heavy trucks.

Pave Tech, Inc. v. Snap Edge Corp., 952 F. Supp. 1284, 1301-02 (N.D. Ill. 1996) (citations omitted).

Thus, the case law is clear that patent claims may use general, and even relative, language, where that language is understood by those in the art, and a patentee is not required to provide a comprehensive description of all circumstances in which infringement may be found, but can instead use general language where a comprehensive description would be impractical.

Microsoft's motion is premised on the theory that "secure" is indefinite because determining whether a particular system is "secure" requires an evaluation of the context. MS Memo. at 2:6-18.. As Exxon Research, Orthokinetics, Chiron and Pave Tech make clear, a claim

[8] A copy of this opinion is attached as Ex. R to the Page Decl.

is not rendered indefinite because its application depends on context, nor because it uses general terms that may apply differently in different circumstances.

3. That reasonable persons might disagree regarding the scope of the claims does not render the claims indefinite.

The fact that reasonable people may disagree regarding the application of a claim term does not render that term indefinite:

> It may of course occur that persons experienced in a technologic field will have divergent opinions as to the meaning of a term, particularly as narrow distinctions are drawn by the parties or warranted by the technology. Patent disputes often raise close questions requiring refinement of technical definitions in light of particular facts. The judge will then be obliged to decide between contending positions; a role familiar to judges. But the fact that the parties disagree about claim scope does not of itself render the claim invalid.

Verve, LLC v. Crane Cams, Inc., 311 F.3d 1116, 1120 (Fed. Cir. 2002). See also Exxon Research, 265 F.3d at 1375 (claims not indefinite even if "expert witnesses, trial courts, and even the judges of this court may disagree"). Thus, the fact that InterTrust and Microsoft have proffered similar, but distinct definitions does not suggest that the claims are indefinite.

4. Claims are not indefinite merely because work is required to determine the scope of the claims, as long as such work is not beyond the abilities of one of ordinary skill.

Patent claims are not indefinite merely because determining their scope requires "trial and error" or experimentation, as long as "undue" experimentation is not required:

> The district court invalidated both patents for indefiniteness because of its view that some "trial and error" would be needed to determine the "lower limits" of stretch rate above 10% per second at various temperatures above 35 degrees C. That was error. Assuming some experimentation were needed, a patent is not invalid because of a need for experimentation. . . . A patent is invalid only when those skilled in the art are required to engage in *undue* experimentation to practice the invention. In re Angstadt, 537 F.2d 498, 503-04, 190 U.S.P.Q. 214, 218 (C.C.P.A. 1976). There was no evidence and the court made no finding that undue experimentation was required.

W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 1557 (Fed. Cir. 1983). The test for "undue experimentation" is whether this would require "ingenuity beyond that to be expected of one of ordinary skill in the art." In re Angstadt, 537 F.2d 498, 503-04 (C.C.P.A. 1976).[9]

[9] This case involved enablement, rather than definiteness, but has been cited by the Federal Circuit (e.g., W.L. Gore, cited above) as describing the undue experimentation test applied to indefiniteness.

C. Microsoft's Two-Part Test for Finding Indefiniteness Has Been Rejected By the Federal Circuit.

Microsoft argues that indefiniteness is determined using a two-part test, including whether the claim is "as precise as the subject matter permits" (MS Memo. at 21:9-10) and argues that InterTrust's use of "secure" was not as precise as possible. Memo. at 12:25-13:23.

Microsoft misstates the law. The Federal Circuit has repeatedly held that § 112(2) does not require that claims be drafted as precisely or specifically as possible:

> Claims are often drafted using terminology that is not as precise or specific as it might be. As long as the result complies with the statutory requirement to "particularly point[] out and distinctly claim[] the subject matter which the applicant regards as his invention," 35 U.S.C. § 112, para. 2, that practice is permissible.

PPG Indus., Inc. v. Guardian Indus. Corp., 156 F.3d 1351, 1355 (Fed. Cir. 1998).

> The trial court was correct to fault the Exxon patents as lacking in specificity in several respects--specificity that in some instances would have been easy to provide and would have largely obviated the need to address the issue of indefiniteness. As is often the case when problems in document drafting lead to litigation, the ideal of precision was not achieved here, and we are left to deal with an imperfect product. While we agree with the trial court that the product was less than perfect, we disagree that the flaws were fatal.
>
> *   *   *
>
> . . . The patentee could easily have cured the ambiguity by adding a single word or phrase to the claims or specification . . . . In fact, much of the extrinsic evidence suggests that the practice in this field of art is to state specifically whether velocity is interstitial or superficial. That practice was not followed in the '982 patent, and the result is that there is some question as to the proper interpretation of the claims. The question we must answer is whether the claims are rendered so ambiguous that one of skill in the art could not reasonably understand their scope. . . .
>
> *   *   *
>
> If this case were before an examiner, the examiner might well be justified in demanding that the applicant more clearly define UL, and thereby remove any degree of ambiguity. However, we are faced with an issued patent that enjoys a presumption of validity. In these circumstances, we conclude that a person of skill in the art would understand the scope of the term U[L], and that the degree of ambiguity injected into the claims by the patentee's lack of precision is therefore not fatal.

Exxon Research, 265 F.3d at 1376, 1383-84.

Microsoft's argument was discussed in an opinion summarizing Federal Circuit law and concluding that the Federal Circuit does not require that patent claims be drafted as precisely as the subject matter permits:

> Citing Amgen, Alcon takes the position that a claim must be as precise as the subject matter permits. The court in Amgen did state that "claims must ... be 'as precise as the subject matter permits.'" 927 F.2d at 1217. That statement, however, was contained in a parenthetical characterization of the holding in Shatterproof Glass Corp. v. Libbey-Owens Ford Co., 758 F.2d 613 (Fed. Cir.), cert. denied, 474 U.S. 976, 88 L. Ed. 2d 326, 106 S. Ct. 340 (1985)), but the court in Shatterproof Glass did not actually state that claims must be as precise as the subject matter permits. Rather, the court there stated that "if the claims, read in the light of the specifications, reasonably apprise those skilled in the art both of the utilization and scope of the invention, and if the language is as precise as the subject matter permits, the courts can demand no more.'" Id. at 624 (quoting Georgia-Pacific Corp. v. United States Plywood Corp., 258 F.2d 124, 136 (2d Cir.), cert. denied, 358 U.S. 884, 3 L. Ed. 2d 112, 79 S. Ct. 124 (1958)) (emphasis added).
>
> Were these the only two cases on the issue, there might be some ambiguity as to whether being as precise as the subject matter permits is a necessary, or merely a sufficient, condition for a claim to pass muster under § 112. Federal Circuit cases do not insist on the kind of precision urged by Alcon. The Federal Circuit has never said that all claims must be made as precise as humanly possible, without exception. In fact, in a case decided after Amgen, the court observed that "claims are often drafted using terminology that is not as precise or specific as it might be. As long as the result complies with the statutory requirement to 'particularly point[ ] out and distinctly claim[ ] the subject matter which the applicant regards as his invention,' 35 U.S.C. § 112, para. 2, that practice is permissible." PPG Indus. v. Guardian Indus. Corp., 156 F.3d 1351, 1355 (Fed. Cir. 1998).
>
> The focus, then, is whether, given the nature of the subject matter, the claim is precise enough to make clear to a person skilled in the art what is claimed. There may be times when, for one reason or another, it is impossible, unnecessary, or undesirable to state a claim in terms of precise, quantified measurements. See, e.g., United States v. Telectronics, Inc., 857 F.2d 778, 786 (Fed. Cir. 1988) (district court erred as a matter of law in holding that if claim were read to mean that electric current must be applied "so as to minimize fibrous tissue formation," it would be invalid under § 112 because it would be "impossible to determine when sufficient minimization takes place to determine what current range is involved"), cert. denied, 490 U.S. 1046, 104 L. Ed. 2d 423, 109 S. Ct. 1954 (1989). That is permissible as long as the dictates of § 112 are met.

Bausch & Lomb, Inc. v. Alcon Labs., Inc., 79 F. Supp. 2d 243, 245 (W.D.N.Y. 1999).

Microsoft misstates Federal Circuit law in precisely the same way as the defendant in Bausch & Lomb. Microsoft's two-part indefiniteness test is wrong.

D. The Undisputed Facts Establish that "Secure" and "Security" Are Definite.

1. Use of the term in the industry.

"Secure" and "security" are widely used in the computer security field. Reiter SJ Decl., ¶¶ 5-7. Acceptance of a term by the industry is evidence that use of the term does not render patent claims indefinite. Rosemount, Inc. v. Beckman Instruments, Inc., 727 F.2d 1540, 1547 (Fed. Cir. 1984); Advanced Cardiovascular Sys., Inc. v. Scimed Life Sys., 96 F. Supp. 2d 1006, 1019 (N.D. Cal. 2000).

2. Use of the term by the defendant in describing its own products.

Microsoft routinely describes its products and features as "secure," both in public documents and in internal documentation. See above, § II A 1(b). The defendant's use of the disputed term supports finding that term not indefinite. Rosemount, 727 F.2d at 1547; Advanced Cardiovascular Systems, 96 F. Supp. 2d at 1019.

3. Use of the term in other patents, including the defendant's patents.

As is described in § II A 3 above, Microsoft's patents use "secure" and "securely" in a manner similar to the InterTrust claims, and these terms are routinely used in claims of third party patents (at least 100 in the past year alone). This supports finding the term to be definite:

> The criticized words are ubiquitous in patent claims. Such usages, when serving reasonably to describe the claimed subject matter to those of skill in the field of the invention, and to distinguish the claimed subject matter from the prior art, have been accepted in patent examination and upheld by the courts.

Andrew Corp. v. Gabriel Electronics, Inc., 847 F.2d 819, 821 (Fed. Cir. 1988).

> Genentech's use of similar terminology without apparent difficulty . . . in its own patent applications, is yet another indication that what is meant by a "useful degree of affinity" is not indefinite. . . .
>
> . . . Genentech's use of the phrase "sufficient affinity" in its own patent application belies its contention that one of ordinary skill in the art would not understand when an antibody has sufficient affinity to be "useful" for therapy.

Chiron Corp., 2002 U.S. Dist. LEXIS 19150, *14-16.[10]

> Indeed, one of Alcon's own witnesses . . . though stating that he did not know what the term "does not substantially inhibit" means in the '607 patent, admitted on cross-examination that several of Allergan's own patents, including some on which Anger himself was named as an inventor, use similar language.
>
> * * *
>
> There was also evidence that Alcon itself has used the word "substantially" in its own patents and in proceedings before the Patent and Trademark Office ("PTO").

Bausch & Lomb, Inc. v. Alcon Labs., Inc., 79 F. Supp. 2d 243, 250 (W.D.N.Y. 1999).

[10] Page Decl., Ex. R.

4. Ability of the Examiner to apply the terms to the prior art.

The PTO Examiners assigned to the InterTrust applications had no difficulty applying the disputed terms (including secure, secure container and protected processing environment) to the prior art. McDow Decl., ¶ 8 and Ex. G. For example, in the Sept. 22, 1998 Notice of Allowance for InterTrust's'019 patent, the Examiner stated that "there is no disclosure [in the prior art Fischer patent] of the recited three secure containers as set forth in the instant claims." He had no difficulty understanding the term "secure containers" or determining whether a "secure container" was disclosed in the prior art. This is one of numerous Patent Office documents quoted in McDow Decl., Ex. G in which Examiners of different InterTrust patents used the term "secure" or a variant and showed that they understood its meaning and were able to apply it.

This supports finding the claims definite. SDS USA, Inc. v. Ken Specialties, Inc., 107 F. Supp. 2d 574, 596 (D.N.J. 2000) (Examiner determining that claim element was found in prior art reference, patent held not indefinite: "SDS accurately surmises from that comment that the 'transfer unit' was readily recognizable to Examiner Crane, and presumably to other skilled professionals, based on mechanisms found in the prior art.").

E. Prof. Mitchell's Analysis Should Be Disregarded, Since He Admittedly Made No Attempt to Understand the Meaning of "Secure" in the Context of the Claims as a Whole.

Prof. Mitchell improperly analyzed the term "secure" in isolation and not in the context of the entire claim in which the term appears. For example, as is described in § II E above, one factor leading Prof. Mitchell to conclude that "secure memory" is indefinite is the fact that the claim does not identify what information other than the digital file is contained in the secure memory, despite the fact that the claim does not require any other information. Prof. Mitchell's explanation revealed that his entire methodology is fatally flawed:

> Q. So, again, sir, is it your testimony that the secure memory recited in '193, claim 1 includes some information other than the digital file?
>
> A. Well, I don't think I have an opinion about it. That sounds like a question about the meaning of the claim, apart from the meaning of the phrase "secure memory."
>
> And, to this point, I haven't really been asked to form a clear

> understanding of the claim and haven't really reflected and done proper study on exactly the question you ask.

Mitchell II 297:2-12.

Thus, Prof. Mitchell believes that "secure memory" is "unclear" in claim 193.1 because (among other things) although the claim indicates a "digital file" is stored in the memory it doesn't identify other information stored in the memory. When asked whether the claim requires such other information, however, he testified that he hadn't studied the claim itself and had no opinion. This testimony was not a momentary aberration:

> Q. Well, does '193, claim 1, require that anything other than the digital file be stored in the secure memory recited in that claim?
>
> THE WITNESS: That sounds like a question about the meaning of the claim rather than a meaning of the phrase "secure memory" to me.
>
> Q. Okay. Does that mean you can't answer the question?
>
> A. To the -- I believe so.

Mitchell II, 298:3-23.

Thus, Prof. Mitchell has no opinion regarding the manner in which "secure memory" is used in the claim, and admits that he doesn't know whether his analysis (e.g., other stored information must be identified) is relevant to the claim, since he hasn't analyzed the claim.

The analysis of indefiniteness begins with the claims themselves:

> Only after a thorough attempt to understand the meaning of a claim has failed to resolve material ambiguities can one conclude that the claim is invalid for indefiniteness. Foremost among the tools of claim construction is of course the claim language itself, but other portions of the intrinsic evidence are clearly relevant, including the patent specification and prosecution history.

All Dental Prodx, LLC v. Advantage Dental Prods., Inc., 309 F.3d 774, 780 (Fed. Cir. 2002).

Prof. Mitchell was not asked to and did not analyze the meaning of the claims and therefore, for example, had no opinion regarding whether one of the elements he felt should be defined as part of "secure memory" was in fact required by the relevant claim. His testimony on indefiniteness was not based on an interpretation of the phrase in the context of the claim. He therefore failed to apply the proper legal standard and his testimony should be disregarded.

F. Microsoft's Evidence, Analogies and Case Support Are Either Irrelevant or Inaccurate.

1. Depositions of third parties.

Microsoft relies heavily on third party testimony regarding the meaning of disputed terms. As is discussed more fully in InterTrust's Motion to Strike, served and filed herewith, these witnesses are not qualified as of ordinary skill in the art, nor have they read the patents, and their testimony is therefore incompetent and should be stricken. If the Court admits this testimony, InterTrust has also included other testimony that establishes that the witnesses understand the disputed terms and can apply them, as well as an explanation of Microsoft's mischaracterization of that testimony. McDow Ex. B, §§ 1(b), 2(b),(c),(d), 3(b),(c).

2. Microsoft's Car and Safe Analogies Are Irrelevant.

Microsoft attempts to convince the Court that "secure" is indefinite because there is no way to know what would be meant if someone characterized a car or a safe as "secure." MS Memo. at 3:13-27; Mitchell Decl., 57-13. These analogies are irrelevant, since the fact that the word "secure" might have no meaning in one context (e.g., a "secure rock") is irrelevant to whether it has meaning in another context in which it is routinely used (e.g., computer security).

3. Microsoft's Argument Relies on Cases that are either Irrelevant or Miscited.

The case discussed at greatest length in Microsoft's brief is Ex Parte Brummer, 12 U.S.P.Q.2d (BNA) 1653 (B.P.A.I. 1989), which Microsoft characterizes as "comparable" to the present case. MS Memo. at 22:13-15. Brummer involved an appeal from a Patent Office decision rejecting patent claims. 12 U.S.P.Q.2d at 1653. The Federal Circuit has warned that the indefiniteness analysis applied to issued patents (e.g., the InterTrust patents) is different than and requires a higher standard than the analysis applied to patent applications (e.g., Brummer). This is the result of the presumption of validity provided to issued patents, a presumption that does not apply to unissued patent applications. Exxon Research , 265 F.3d at 1380. See also, Solomon v. Kimberly-Clark Corp., 216 F.3d 1372, 1378-79 (Fed. Cir. 2000) (different standards applicable to indefiniteness analysis during patent examination and during litigation on issued patent means that evidence properly considered to establish indefiniteness during examination should not be considered to establish indefiniteness in litigation).[11]

The difference between the indefiniteness standard applied to patent applications and the standard as applied to issued patents is illustrated by the differing outcomes in Brummer and Orthokinetics, cases each involving patent claims drafted in the context of the environment in which the patented item would be used. In Orthokinetics, claims were found definite despite the fact that those claims included an element described as dimensioned so as to fit into an automobile. The Federal Circuit noted that different dimensions would be required for different automobiles, but upheld validity of the claims nevertheless. Orthokinetics, 806 F.2d at 1576.

Microsoft also discusses In re Lechene, 277 F.2d 173 (C.C.P.A. 1960), at some length, arguing that an element discussed in that case ("stiff") is similar to "secure." MS Memo. at 22:6-12. Not only does this case involve an unissued patent application, the decision has nothing to do with definiteness under § 112(2). Instead, the opinion holds that claims were properly rejected as obvious based on a prior art reference. The opinion happens to use the word "indefinite," but in a context having nothing to do with § 112(2).

Microsoft relies on a 1938 case (General Electric Co. v. Wabash Appliance Corp., 304 U.S. 364 (1938)) for the proposition that "claim indefiniteness is particularly problematic where it derives from 'conveniently functional language at the exact point of novelty.'" MS Memo. at 23:7-8. That holding is irrelevant, however, since it involved a principle of claim construction (apparatus claims cannot include functional limitations) that was expressly overruled by the adoption of 35 U.S.C. § 112(6), and since Microsoft makes no argument that InterTrust's claims are indefinite based on inclusion of "functional" language.

Microsoft tries to shoehorn this into an indefiniteness argument by citing Dr. Reiter's testimony for the proposition that "security" is an "essential aspect" of the invention, and arguing that Exxon Research (cited above) stands for the proposition that it is "fatal for limitations critical to patentability to be indefinite." MS Memo. at 23:13-14.

This argument is wrong. First, Microsoft's characterization of Dr. Reiter's testimony is

[11] Microsoft's reliance on In re Cohn, 438 F.23d 989 (C.C.P.A 1971) (MS Memo. at 21:23-25) is misplaced for the same reason, since Cohn also involved an unissued patent application..

completely inaccurate. Reiter SJ Decl., ¶¶ 52-53. Second, Exxon Research contains no such holding. Instead, in Exxon Research the Federal Circuit distinguished an earlier decision on a number of grounds, one of which was the fact that the patent specification in the earlier case had characterized a limitation as critical to patentability, a factor not present in the Exxon Research case. The Federal Circuit noted that the Court of Customs and Patent Appeals had held that it was "not fatal for an applicant to express noncritical limitations with regard to factors such as time or quantity in functional rather than numerical terms." Exxon Research, 265 F.3d at 1379, citing In re Caldwell, 319 F.2d 254, 258 (C.C.P.A. 1963). The Federal Circuit neither stated nor implied that a different indefiniteness standard applies to "critical" limitations.

G. "Protected Processing Environment" and "Host Processing Environment" Are Not Indefinite

1. Protected Processing Environment.

Microsoft's discussion of Protected Processing Environment ("PPE") ignores extensive discussion in the specification. Thus, Microsoft complains that PPE is defined in terms of two other defined terms (HPE and SPE), and that defining one coined term with two other coined terms is "an unhelpful exercise." MS memo. at 18:11-13. Microsoft ignores, however, the specification's detailed description of SPEs and HPEs. Reiter SJ Decl., ¶¶ 39-40, Ex. G.

In addition, Microsoft passes lightly over the figures: "General reference is then made to the PPE in the 'Brief Description of the Drawings' but no meaningful discussion . . . ." MS Memo. at 17:25-26. This statement is false. Several of the drawings are explicitly described as relating to PPEs, and the patents contain dozens of pages describing these drawings. Reiter SJ Decl., ¶ 39-40 and Ex. G. Microsoft ignores all of this.

Prof. Mitchell finds "protected processing environment" indefinite based on his ten-part test. As with "secure," however, he has no difficulty understanding what the term means:

> The protected processing environment likewise shields the information it contains, again through the use of rules governing the access and use of the information. Information apparently cannot be used or accessed by anyone or anything without satisfaction of those associated, governing rules.

Mitchell Decl., 50:20-24.

Again, the issue is not whether InterTrust agrees with Prof. Mitchell's definition. For indefiniteness, the question is whether one of ordinary skill in the art can understand the term. Prof. Mitchell clearly has the ability to do so. His quibbles regarding the failure of the claims to specify every feature that is present (or absent) in a protected processing environment raise the same issues discussed above in connection with his application of his ten-part test to "secure."

2. Host Processing Environment.

Microsoft presents no evidence for its claim that "Host Processing Environment" is indefinite, except that the term was not in general use. Prof. Mitchell does not discuss this term.

Instead of evidence, Microsoft mischaracterizes the InterTrust patents, arguing that the term "host processing environment" is found in only a couple of locations in the patents, and that these locations do not clearly explain what the term means. MS Memo. at 19:7-24.

Microsoft's statement is highly misleading. Although the '900 patent discusses "host processing environments" in only a few locations, it contains extensive description of "HPEs." Reiter SJ Decl., ¶¶ 41-42. Microsoft was aware that the patent uses the acronym "HPE" to refer to Host Processing Environment (MS Memo. at 17:9), but chose to disregard the specification discussion of "HPEs" in favor of arguing that "host processing environments" were only discussed in a few places. This appears to be a deliberate attempt to mislead the Court.

H. The Foundational InterTrust Patent Application is Effectively Incorporated By Reference.

Microsoft seeks a ruling that would effectively invalidate three issued U.S. Patents as a result of a clerical error committed by the Patent Office. Those patents incorporate the original InterTrust application by reference, a procedure explicitly authorized by patent law. Microsoft's sole basis for complaint is that the application number was not later replaced by an issued U.S. patent number. Microsoft implies that this is improper because the original application was not available to those attempting to evaluate the later patents, but this is false, since the earlier application may be obtained from the Patent Office at minimal or no cost. No U.S. Patent has ever been invalidated based on the failure to replace an incorporated by reference application number with a patent number, and Microsoft carries a burden of establishing this issue by clear and convincing evidence. InterTrust therefore seeks summary judgment on this issue.

According to Microsoft, the original InterTrust patent application is not properly incorporated by reference into three of the later-filed InterTrust patents. Microsoft characterizes the original application as "essential material" to these later patents. Microsoft Memo. at 12:7-9.

A patent that fails to incorporate "essential material" is invalid for lack of enablement. Quaker City Gear Works, Inc. v. Skil Corp., 747 F.2d 1446 (Fed. Cir. 1984). For this reason, Microsoft must establish the failure to incorporate by clear and convincing evidence. Intel Corp. v. Via Technologies, Inc. 319 F.3d 1357, 1366 (Fed. Cir. 2003).

The three InterTrust patents incorporate the earlier application by reference. McDow Decl., ¶ 11. Such incorporation is authorized by the MPEP. See MPEP § 608.01(p), reproduced in the Declaration of Karna J. Nisewaner ("Nisewaner Decl."), ¶ 4 and Ex. 1.

It has long been settled that a patentee's § 112 obligations may be met by materials incorporated by reference, as long as those materials are reasonably available to the public:

> We recognize that, subject to compliance with 35 USC 112 and 132, the disclosure in a patent application may be deliberately supplemented or completed by reference to . . . disclosure in earlier or concurrently filed copending applications, . . . or, in general, to "disclosure which is available to the public," . . . . As the expression itself implies, the purpose of "incorporation by reference" is to make one document become a part of another document by referring to the former in the latter in such a manner that it is apparent that the cited document is part of the referencing document as if it were fully set out therein.

In re Lund, 376 F.2d 982, 989 (C.C.P.A. 1967) (citations omitted).

> That total incorporation by reference cannot be accomplished under 112 is apparent from the reading of Lund, Heritage and Stauber. It is limited to reference to material available to the public. This would exclude secret or privileged materials as in the case of some abandoned patent applications. It is reasonable also to exclude materials which are not easily available to the public or the Patent Office. This would include unpublished dissertations and theses, obscure foreign publications and publications to which there are no available English translations.

General Electric Co. v. Brenner, 407 F.2d 1258, 1262-63 (D.C. Cir. 1968).

According to the MPEP, pending or abandoned applications are readily available. Nisewaner Decl., ¶ 4, Ex. 1. The InterTrust application may be obtained from the Patent Office. Nisewaner Decl., ¶¶ 6-9. In addition, the text of the application may be obtained for free in a matter of minutes through the PTO's on-line service. Nisewaner Decl., ¶¶ 10-11. Microsoft's implication that incorporation of the original InterTrust application by reference was improper because that application is unavailable is false: the application is readily available to the public.

Microsoft argues that the reference to the incorporated InterTrust application should have been replaced with a reference to an issued patent. MS Memo. at 12:19-24. According to MPEP § 608.01(p), the examiner is supposed to replace an application number with the issued patent number. Microsoft cites no support for the argument that issued patents should be invalidated because of what amounts to a clerical mistake by the Patent Office, and it does not appear that any issued patent has ever been invalidated based on this theory. Microsoft cannot possibly carry its burden of showing invalidity by clear and convincing evidence, given the indisputable fact that the application is readily available at low cost. Summary judgment that the application was properly incorporated by reference, and the three patents are therefore not invalid for failure to include essential material is therefore proper.

Even if the foundational application had not been properly incorporated by reference, the later patents contain significant description of the allegedly indefinite terms, description that Microsoft simply ignores. Reiter SJ Decl.,¶ 43, Ex. H.

Microsoft has not carried its burden of establishing that these disclosures lack sufficient information for one of ordinary skill in the art to understand the claims of those patents in light of their specifications. Summary judgment should be entered against Microsoft on this issue.

IV. CONCLUSION

InterTrust respectfully requests that the Court deny Microsoft's motion for summary judgment and grant InterTrust's cross-motion for summary judgment.

Dated: April 7, 2003

DERWIN & SIEGEL, LLP

By:
DOUGLAS K. DERWIN
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE (State Bar No. 178960)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
RICHARD D. MC LEOD (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	CASE NO. C01-1640 SBA (MEJ) **MICROSOFT'S MARKMAN BRIEF**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	The Honorable Saundra B. Armstrong

TABLE OF CONTENTS

CASES

STATUTES/OTHER

I. INTRODUCTION

The claims must be read in light of the entire 900+ page "Big Book" patent application and, in particular, its 115 page "Summary of the Invention." This Summary of the Invention makes literally hundreds of statements touting the "important," "fundamental," "critical," and required features, capabilities and purposes of the "present invention." The Summary further defines this "invention" (which it expressly names "VDE") by distinguishing it from the allegedly "limited" and rigid solutions of others. All of these are required aspects of the "present invention," not merely optional features of a "preferred embodiment." As such, the claims must be read to include these "invention" features.

A. A Valid Claim Must Reflect This "Invention"

The Big Book's Summary of the Invention is InterTrust's elephant in the corner. The claim constructions urged by InterTrust are devoid of any of the required features of the "invention." InterTrust acts as if this "invention" simply did not exist. For example, the Big Book touts that VDE is able to prevent (not merely detect) all unauthorized access to protected content. Yet, InterTrust uniformly ignores this core promise of VDE security in its claim construction proposals, and instead urges that merely detecting misuse of content is sufficient.

InterTrust's whole approach is wrong. To ignore a patent's described "invention" when construing a patent claim, is contrary to patent law. "What is claimed by the patent application must be the same as what is disclosed in the specification; otherwise the patent should not issue." Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., 535 U.S. 722, 736 (2002). Thus, "it is fundamental that claims are to be construed in the light of the specifications and both are to be read with a view to ascertaining the invention." Adams v. United States, 383 U.S. 39, 49 (1966) (holding that patent claims required what the patent identified as an "object" of the "invention," even though the claims did not expressly recite that feature). Here, the Big Book's Summary of the Invention is critical to "ascertaining the invention."

B. These Twelve Claims Do Invoke This "Invention"

InterTrust's patent claims invoke the required features of the alleged "invention" in at least three ways.[1]

VDE Claim Terms: First, many of the key claim terms are VDE terms having special meanings in the VDE context. For example, the Big Book uses several general-sounding, functional terms (often a coined phrase) as short-hand labels for specific VDE mechanisms, such as "control," "container," "protected processing environment," and "virtual distribution environment." In these patents, a "control" is not whatever can exercise some kind (any kind) of control over something else; a "container" is not whatever can contain something; a "protected processing environment" is not any processing environment which is protected; and a "virtual distribution environment" is not any distribution environment which is virtual. Rather, these terms have special VDE meanings. For example, the Big Book defines its "virtual distribution environment" as a special breed: "The present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use." ('193 2:24-27). These claim terms must be construed in their specific VDE sense, not some general sense divorced from the described "invention." (See Maier Decl. at 21-35.)

Vague Claim Terms: Second, most of the key claim terms are quite vague. These terms would deprive the claims of required clarity unless they are refined in light of the disclosed "invention." For example, ten of the mini-Markman claims use the terms "secure," "securely," and/or "protected." These claims do not specify how to distinguish a secure [something] from a non-secure [something], etc. Whether a "container" is "secure," for example, depends on the context, such as what is being protected, against what threats, for how long, and to what degree. (See Tran Decl. (Public) (assembling references); Keefe Decl. (assembling testimony: e.g., Shear Depo. at 100:19-101:23; Sibert Depo. at 97:20-25, 29:8-11); and the first Declaration of John

[1] Any claim that fails to invoke its specification's "invention" is invalid under 35 U.S.C. § 112, ¶ 1's "written description" requirement and ¶ 2's "regards as the invention" requirement. (See infra, Section V).

Mitchell (filed March 17, 2003).) As the claims do not expressly provide this required context, resort must be had to the disclosed "invention."[2] Many other claim terms also are sorely in need of definition from the specifications. (Cf. InterTrust Br. at 9:2-18).

VDE Claim Promises: Third, a core "invention" promise is the ability to prevent unauthorized access to (and use of) protected digital content notwithstanding myriad threats—identified in the Big Book—attempting to break or bypass that protection. (E.g., '193 221:19 et seq.) Each of the mini-Markman claims invokes this core VDE promise by promising to protect some content, process, and/or component. These promises of protection are unqualified. The claims identify no threat against which their promised protections are ineffective. The Big Book describes only one system for providing such "true" protection against these threats, and that is the complete VDE "invention." In other words, by requiring the promised protections supposedly afforded by the "invention," these claims invoke the required features of that "invention."

C. These Claims Demand Precise Constructions, True To The "Invention"

As InterTrust says, its proposed constructions are simple. They are simple, however, because (1) they are unfettered by the disclosed "invention" and its required capabilities and features touted in the Big Book's Summary of the Invention, (2) they treat the claims' specific VDE terms as general, non-VDE terms, (3) they ignore what each claim promises, and (4) they often are so vague as to be essentially meaningless.

InterTrust challenges Microsoft's constructions as complex. They are complex, because they honor precisely what the Big Book describes as the many required features of the "present invention." A proper construction of these claims necessarily is lengthy due to the sheer number of features the Big Book identifies as being "important" to its "invention." These required features are not "detailed limitations from specified embodiments," as charged by InterTrust (InterTrust Br. at 1:19-20), but rather the self-described "important" features of the "invention."

Simplicity and brevity are worthy goals in claim construction. But, they do not trump clarity and accuracy. Skilled persons faced with these claims would not dismiss any required

[2] Here, InterTrust's specification is internally inconsistent and, in some ways, makes the scope of the claims even less clear. Consequently, Microsoft has moved for summary judgment of claim indefiniteness.

aspect of the Big Book's "invention." The sheer size of the Big Book should not frustrate the rules of claim construction, leave the public or jury guessing about a claim's precise boundaries, or divorce the claims from what the patent applicants touted as their "present invention."

II. SUMMARY OF ACCOMPANYING DECLARATIONS

The parties agree that this subject cannot be fully addressed in a 40-page brief. This Brief addresses some important features of the "invention" and some of the primary claim construction disputes. It is supplemented by the JCCS, and by the following declarations:

VDE's Features: The Declaration of Prof. David Maier, of Oregon Graduate Institute, describes the Big Book's "invention" and its mandatory features. To illustrate the operation of this "invention," he also explains the Big Book's only detailed example of how VDE handles a request to read protected content. Prof. Maier also describes some of the inconsistencies in the Big Book, including some that contradict passages cited by InterTrust.

"Security" And The Claims: Prof. John Mitchell, of Stanford, submitted a report on Microsoft's pending motion for summary judgment of claim indefiniteness. That report also pertains to claim construction. It explains how the label "secure" is "multi-dimensional, highly contextual, relative (i.e., a matter of degree), and subjective unless objectively defined." In his second Declaration, Prof. Mitchell explains how the "security" protections promised by the "invention" would have affected a skilled person's understanding of certain claim terms.

Prosecution History: Mr. Alexander summarizes portions of the Patent Office files for these patents and explains the relationships between the patents. Included is the Patent Office's statement (set forth with its reasons for allowing the '193 patent to issue) that InterTrust had filed "a series of applications generally relating to a virtual distribution environment."

Deposition Testimony: In opposing Microsoft's motion to stay certain discovery, InterTrust argued that the parties' own uses of the claim terms are important to claim construction. (InterTrust Opp. to Microsoft's Motion for Stay at 9-10 & n. 9 (October 1, 2002).) Microsoft has since deposed several InterTrust employees, former employees, licensees, and licensee candidates, as well as InterTrust's expert, Prof. Reiter. Their testimony confirms that many key claim terms lack any precise meaning outside of VDE. Ms. Keefe's Declaration collects some of this testimony.

Documentary Evidence: Two Declarations by Xuan-Giang Tran submit documentary evidence supplementing the parties' joint submission of intrinsic evidence.

III. THE BIG BOOK'S "INVENTION"

Microsoft asks the Court to construe each claim as requiring the disclosed "invention," as it has been distilled in Microsoft's global "claim as a whole" construction. (JCCS Exh. A, Row 86). Some of the important aspects of this "invention"—aspects which the Big Book cites to distinguish prior systems—are summarized below. (See also Maier Decl. at 5-14).

Data Security and Commerce World: The overall purpose of the "invention's" Virtual Distribution Environment (VDE) is for securing, administering, and auditing all security and commerce digital information within its multi-node "world." VDE guarantees to all participants in this VDE world that it can limit all access to, and use of, such security and commerce information, to authorized activities and amounts.

> "The **present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use.** VDE also features fundamentally important capabilities for managing content that travels 'across' the 'information highway.'" ('193 2:24-28)
>
> "**The present invention** can provide a "unified," efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as **a single standard for electronic rights protection, data security, and electronic currency and banking.**" ('193 7:9-14)
>
> "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. **VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users.**" ('193 4:48-55)

(Alexander Decl. Exh. D at 24-1(C), 24-9(C), 24-1(F).) (Emphases added throughout this Brief, unless otherwise noted).

Comprehensive Range of Functions: The Big Book distinguishes its comprehensive "invention" from supposedly "limited" traditional systems that addressed only some aspects of data security and commerce.

> "**Content providers and distributors have devised a number of limited function rights protection mechanisms to protect their rights.** Authorization passwords and protocols, license servers, 'lock/unlock' distribution methods, and non-electronic contractual limitations imposed on users of shrink-wrapped software are a few of the more prevalent content protection schemes. In a commercial context, **these efforts are inefficient and limited solutions.**" ('193 3:1-9)

> "**Despite the attention devoted** by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies **to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems.**" ('193 2:13-22)

(Alexander Decl. Exh. D at 24-7(K), 24-4(V).)

User-Configurable: The "invention" governs access to and use of protected information with executable VDE "controls." These VDE controls are not built-in, fixed mechanisms. Rather, VDE allows its participants to create, modify, and merge these VDE controls, partly through a VDE-controlled negotiation process. For example, VDE purports to enable[3] a consumer to place limits on the amount of time or money that a participant (whether human or machine) can spend using the protected content, subject only to other users' "senior controls."

> "The **inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention.**" ('193 2:11-13)

> "The **configurability provided by the present invention** is particularly **critical for supporting electronic commerce,** that is enabling businesses to create relationships and evolve strategies that offer competitive value. **Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce** products (and services) that meet both basic requirements and evolving needs of most commerce applications." ('193 16:41-48)

[3] Throughout this brief, Microsoft describes various features described in the Big Book and other InterTrust patents. By reiterating what InterTrust patent documents say, Microsoft does not imply that those documents actually described a working system that could accomplish what they promised. In other words, Microsoft addresses what the patents purported to describe, not whether they actually enabled anything.

(Alexander Decl. Exh. D at 24-4(V), 24-4(W).)

Flexible: The Big Book further distinguishes its supposedly flexible system from rigid systems. For example, rather than requiring a VDE user to purchase an entire, pre-defined content package (e.g., an entire movie), the "invention" can permit a VDE user to purchase only user-defined increments of that information (e.g., her favorite scenes).

> "**Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.** VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, **VDE includes features that . . . support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments** such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section. . ." ('193 21:43-53; 22:32-38)
>
> "**VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed functionality.**" ('193 9:67-10:9)

(Alexander Decl. Exh. D. at 24-1(Q), 24-10(G).)

The VDE Mechanisms: The Big Book describes various embodiments for providing these (and other) core "invention" capabilities. It describes no embodiment, however, that is said to achieve these "invention" capabilities without using at least the described VDE controls, VDE "secure containers," and VDE "secure processing environments." On the contrary, the Big Book emphasizes that the design of its VDE components is an "Important Feature" of the "invention." (See Alexander Decl. Exh. D at 24-1(S) ('193 21:43-45, 34:25-30).)

None of the above capabilities and components is merely an optional characteristic of some embodiment. They are core, defining features of the "present invention."

IV. THE "INVENTION" PROMISES THAT IT IS ABLE TO PREVENT ALL ACCESS TO AND ALL USE OF PROTECTED CONTENT EXCEPT AS AUTHORIZED BY VDE CONTROLS

Another aspect of the VDE "invention" is particularly important to claim construction.

Non-Circumventable: VDE claims that the protections it promises cannot be bypassed, i.e., they are not circumventable. Rather, VDE intercepts attempts by any and all users (including would be misusers) to access or use protected information. It thereby "ensures" that the VDE controls designed to govern such access and use, in fact do so, and that all unauthorized access and use is "prevented." (See Alexander Decl. Exh. D at 24-5(A), 19(K) ("VDE enables parties ... to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled" ('193 6:18-31); "the present invention ensures that content control information can be enforced." ('193 46:4-8).) As stated at '193 11:8-11:

> "**All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used.**

This non-circumventable "access control" is critical to a proper construction of these patent claims. The secrecy of digital information (e.g., an electronic vote) may be protected by encrypting it. Encryption does not, however, provide full protection. (See Reiter Depo. at 49:7-14, 53:1-11, 55:13-16.) It does not prevent an attacker from deleting the content, or altering it, copying it, tracing it, or moving it. Thus, as the "invention" prevents all types of misuse, it does more than merely encrypt content. Specifically, VDE promises those who entrust their valuable content to it, that VDE is able to prevent all forms of unauthorized access to the content. By preventing unauthorized access, VDE prevents all unauthorized uses, including misuses which are not prevented by mere encryption (such as deleting, altering, copying, or moving the content). In other words, VDE promises a second layer of protection—a bank vault like "access control" that cannot be circumvented:

> "The virtual distribution environment 100 **prevents use** of protected information except as permitted by the "rules and controls" (control information). ('193 56:26-28)

> "As mentioned above, virtual distribution environment 100 'associates' content with corresponding 'rules and controls,' and **prevents the content from being used or accessed** unless a set of corresponding 'rules and controls' is available." ('193 57:18-22)

> "Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information **to prevent this information from ever becoming available to users even in encrypted form.**" ('193 166:59-64)

InterTrust's expert, Prof. Reiter, has agreed that the '193 Patent says that VDE is able to prevent physical access to protected content. (See Reiter Depo. at 55:17-60:1). Nevertheless, InterTrust's proposed constructions uniformly disregard this core VDE promise.

This "access control" capability of the "invention" is critical to a proper understanding of the most important claim terms in dispute. For example, various claims promise protections against unauthorized "use" or "copying" of protected content. InterTrust's proposed constructions of "use" and "copy" assume that only encryption is used to protect the content. Thus, per InterTrust, "use" and "copy" must mean only those types of uses and copying which can be prevented with encryption. That construction is wrong because that assumption is wrong. VDE promises content access control, not just encryption. In this VDE context, the claims protect against all forms of use and copying, not just those which require decryption.

V. <u>CLAIMS CONSTRUCTION LAW</u>

A. General Claim Construction Legal Analysis

The statutory measure of a patent's scope is its patented "invention," which is required to be set forth "distinctly" in the patent claims. 35 U.S.C. § 112, ¶ 2. There are statutory requirements to help ensure that what is claimed is the "invention." One is that a patent may claim as its invention only subject matter that "the applicant regards as his invention." 35 U.S.C. § 112, ¶ 2. Another is that a patent may claim only the "invention" described in the patent application's written description. 35 U.S.C. § 112, ¶ 1. These requirements, coupled with the public notice function of a patent, explain why it is fundamental that "claims are to be construed in the light of the specifications and both are to be read with a view to ascertaining the **invention**." <u>Adams</u>, 383 U.S. at 49; <u>see also Vitronics Corp. v. Conceptronic, Inc.</u>, 90 F.3d 1576 (Fed. Cir. 1996) ("the public is entitled to rely" on the instrinsic evidence for notice as to what the patent does and does not cover). Last year the Supreme Court confirmed this necessary link: "What is claimed by the patent application must be the same as what is disclosed in the specification." <u>Festo</u>, 535 U.S. at 736 .

The standard claim construction rules are set forth in <u>Vitronics</u>. <u>See</u> 90 F.3d at 1582-83 (citing <u>Markman v. Westview Instrs., Inc.</u>, 52 F.3d 967 (Fed. Cir. 1995), <u>aff'd</u>, 517 U.S. 370

(1996)). See also Schering Corp. v. Amgen Inc., 222 F.3d 1347, 1353 (Fed. Cir. 2000) (interpreting patent terms as one of skill in the art at the time of the application would understand them). In ascertaining the patent's "invention," the claims' language is of primary importance. See Vitronics, 90 F.3d at 1582. However, courts must look also to both "intrinsic" and "extrinsic" evidence. See Lacks Indus. v. McKechnie Vehicle Components USA, Inc., 2003 U.S. App. LEXIS 4471, at *14 (Fed. Cir. Mar. 13, 2003) (for claim construction, "we begin with an examination of the intrinsic evidence, i.e., the claims, the other portions of the specification, and the prosecution history (if in evidence). Courts may also review extrinsic evidence in construing a claim. Additionally, dictionary definitions, although extrinsic, may be used to establish a claim term's ordinary meaning.") (internal citations omitted) (See Tab B, hereto).

Among the intrinsic evidence, "the specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." Vitronics, 90 F.3d at 1582.[4] "One purpose for examining the specification is to determine if the patentee has limited the scope of the claims." Watts v. XL Sys., Inc., 232 F.3d 877, 882 (Fed. Cir. 2000). In making this determination, however, courts must refrain from reading in unnecessary limitations from the specification into the claims. See Comark Communications, Inc. v. Harris Corp., 156 F.3d 1182, 1186 (Fed. Cir. 1998).

Recent Federal Circuit decisions have proposed that a way to help ensure this balance is to first look to the "ordinary meaning" of claim terms, then review the specification and prosecution history to ensure that it is appropriate to apply the "ordinary meaning." See Texas Digital Sys., Inc. v. Telegenix, Inc., 308 F.3d 1193, 1201-04 (Fed. Cir. 2002) (construing, *inter alia*,

[4] InterTrust's brief erroneously implies that a patent specification's purpose is limited to providing an enabling disclosure. (InterTrust Br. at 4:17-18). However, Federal Circuit precedent makes clear that even when the claims are plain on their face, it is necessary to consult the specification during claim construction. See Prima Tek II, L.L.C. v. Polypap, S.A.R.L., 318 F.3d 1143, 1148 (Fed. Cir. 2003) ("After identifying the plain meaning of a disputed claim term, the court examines the written description and the drawings to determine whether use of that term is consistent with the ordinary meaning of the term."); Texas Digital Sys., Inc. v. Telegenix, Inc., 308 F.3d 1193, 1204 (Fed. Cir. 2002) ("the intrinsic record also must be examined in every case").

"activating" in accordance with the ordinary meaning, consistent with the intrinsic evidence, and not accepting patentee's broader proposed construction). Under this approach, the first challenge is to determine whether there is an "ordinary meaning." Id. To do so, courts look to the plain language of the claims and determine whether **appropriate** dictionaries or treatises provide guidance as to the meaning of the terms. See id. at 1202-04; cf. Hoechst Celanese Corp. v. BP Chems. Ltd., 78 F.3d 1575, 1580 (Fed. Cir. 1996) ("a general dictionary definition is secondary to the specific meaning of a technical term as it is used and understood in a particular technical field."). Courts then "must" examine the intrinsic record to ensure consistency with the "ordinary" meaning; "[i]ndeed, the intrinsic record may show that the specification uses the words in a manner clearly inconsistent with the ordinary meaning . . . [and, in such a case, the "ordinary meaning"] must be rejected." Texas Digital, 308 F.3d at 1204. The intrinsic record may also be used to select from among various "ordinary meanings." Id. at 1203. Cf. Rexnord Corp. v. Laitram Corp., 274 F.3d 1336, 1345 (Fed. Cir. 2001) (observing that the "Summary of the Invention" section of the written description is "a pertinent place to shed light upon what the patentee has claimed.").

In certain instances, a "plain meaning" simply does not exist. See, e.g., Lacks, 2003 U.S. App. LEXIS at *16 ("the dictionary definitions do not provide a plain meaning"); J.T. Eaton & Co. v. Atlantic Paste & Glue Co., 106 F.3d 1563, 1568 (Fed. Cir. 1997) (disputed claim term "is a term with no previous meaning to those of ordinary skill in the prior art. Its meaning, then, must be found somewhere in the patent.").

Even where an ordinary meaning exists, there are several situations in which the Federal Circuit has recognized that the "ordinary meaning" is not appropriate. See, e.g., CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366 (Fed. Cir. 2002) ("a court may constrict the ordinary meaning of a claim term in at least one of four ways"). Significant precedent establishes at least the following ways, relevant to the claims in this mini-Markman proceeding, in which claim terms should not be afforded their "ordinary meaning":

1) **To Provide Clarity**: A claim term will not have its ordinary meaning **if the term "chosen by the patentee so deprive[s] the claim of clarity" as to require resort to the other**

intrinsic evidence for a definite meaning." Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1374-75 (Fed. Cir. 2003) (holding that "automation code" "is so broad as to lack significant meaning" and, thus, court limited claim to the only disclosed embodiment). See generally NeoMagic Corp. v. Trident Microsystems, Inc., 287 F.3d 1062, 1071-72 (Fed. Cir. 2002) (restricting claim to a particular type of electrical "coupling," based on specification, although dictionary definition was more general); Watts, 232 F.3d at 882-83 (holding claim term was not "clear on its face," and limiting the claim to a particular embodiment which was described as a feature of the "present invention"); Ethicon Endo-Surgery, Inc. v. U.S. Surgical Corp., 93 F.3d 1572, 1579 (Fed. Cir. 1996) (limiting "pusher assembly" to that described in drawings when the term was "ambiguous" and the specification provided "minimal guidance"); North Am. Vaccine, Inc. v. American Cyanamid Co., 7 F.3d 1571, 1576 -77 (Fed. Cir. 1993) (limiting unclear claim term "linkage to a terminal portion" to linkage at only one terminal as described in the specification).

2) Express or Implied Definition in Patent: "[T]he claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer and **clearly set forth a definition of the disputed claim term in either the specification or prosecution history.**" CCS Fitness, 288 F.3d at 1366-67 (citing Johnson Worldwide Assoc. v. Zebco Corp., 175 F.3d 985, 990 (Fed. Cir. 1999); Rexnord Corp. v. Laitram Corp., 274 F.3d at 1342). The patent applicant's definition need not be express; when a patentee uses a claim term throughout the entire patent specification, in a manner consistent with only a single meaning, he has defined that term "by implication." Bell Atlantic Network Servs., Inc. v. Covad Communications Group, Inc., 262 F.3d 1258, 1268, 1273 (Fed. Cir. 2001) (limiting claim term "mode" to one type of mode, as the patent "defined the term 'mode' by implication" throughout the specification). See generally Abbot Labs. v. Novopharm Ltd., 2003 U.S. App. LEXIS 5357, at **13-18 (Fed. Cir. Mar. 30, 2003) (construing "a co-micronized mixture of particles of [x and y]" to mean "co-micronization of a mixture consisting essentially of only [x and y]" based on definition provided in specification) (emphasis in original) (See Tab A, hereto); Multiform Desiccants, Inc. v. Medzam, Ltd., 133 F.3d 1473, 1477-78 (Fed. Cir. 1998) (observing that an inventor may bestow "a special meaning to a term in order to convey a character or property or nuance relevant to the particular invention").

3) Important to "Invention": The court will limit the ordinary meaning where the specification describes a particular feature or embodiment as "**important to the invention.**" E.g., Toro Co. v. White Consol. Indus., 199 F.3d 1295, 1301 (Fed. Cir. 1999) (limiting claim term to a unitary structure based in part on statements in the specification describing that structure as "important to the invention"). Cf. Scimed Life Sys. v. Advanced Cardiovascular Sys., 242 F.3d 1337, 1342-43 (Fed. Cir. 2001) (limiting claim term "lumen" to "coaxial lumen" in part because the specification characterized the coaxial configuration as part of the "present invention.")

4) Distinguishing Prior Art: "[A] claim term will not carry its ordinary meaning if the intrinsic evidence shows that the **patentee distinguished that term from prior art on the basis of a particular embodiment**," CCS Fitness, 288 F.3d at 1366-67 (citing Spectrum Int'l Inc. v. Sterilite Corp., 164 F.3d 1372, 1378 (Fed. Cir. 1998) (narrowing a claim term's ordinary meaning based on statements in intrinsic evidence that distinguished claimed invention from prior art). See generally Rheox, Inc. v. Entact, Inc., 276 F.3d 1319, 1325-26 (Fed. Cir. 2002) (restricting claim to a particular type of phosphate in light of prosecution history disclaimer of other types of phosphate, despite specification's description of some of the "disclaimed" types of phosphate); Innovad Inc. v. Microsoft Corp., 260 F.3d 1326, 1332 (Fed. Cir. 2001) (restricting claim to devices that did not have keypads, based on specification and prosecution history statements distinguishing prior art).

5) Express Disclaimer: A claim term will not carry its ordinary meaning if the intrinsic evidence shows the patentee **"expressly disclaimed subject matter."** CCS Fitness, 288 F.3d at 1366-67. See generally Scimed, 242 F.3d at 1342-44 (limiting claim term based in part on statements in the specification indicating the invention "excludes" other structures); Ballard Med. Prods. v. Allegiance Healthcare Corp., 268 F.3d 1352, 1361-62 (Fed. Cir. 2001) (finding an explicit disclaimer of "pressure valves" and "dynamic seals" where patentee asserted that his invention, in contrast to such prior art, comprised "vacuum valves" and "static seals").

As shown above, District Courts, the Federal Circuit, and the Supreme Court frequently determine the scope of the "invention" described in the patent specification in the course of determining scope of the issued claims. Where there is a possible disconnect between the disclosed "invention" and the claims, the Federal Circuit normally will construe the claims narrowly, rather than invalidate the claims. See, e.g., Tate Access Floors, Inc. v. Interface Architectural Res., Inc., 279 F.3d 1357, 1367 (Fed. Cir. 2002) ("claim language should generally be construed to preserve validity, if possible"); Schering Corp., 222 F.3d at 1353-54 (limiting claim to one subspecies, as that was all that was described and enabled by specification). However, where the claim on its face is clear and there is no link or "hook" at all in the claim for what the patent described as the "invention," then the Court may construe the claim broadly, but invalidate it under Sec. 112, ¶ 2 or ¶ 1. See, e.g., Cardiac Pacemakers, Inc. v. St. Jude Med., Inc., 296 F.3d 1106, 1114 (Fed. Cir. 2002) ("where the specification fails to disclose structure corresponding to the claimed function, [preserving validity] is impossible [so] the claims are invalid."); Tate Access, 279 F.3d at 1372 ("where claim language is clear we must accord it full breadth even if the result is a claim that is clearly invalid.").

B. Other Claim Construction Issues In This Case

1. Incorporation f One Pending Application Into Another By Reference

Three InterTrust patents (the '683, '721, and '861) purport to incorporate the Big Book by reference to the unpublished patent **application**. (See '721 at 1:7-19; '683 at 1:11-23; '861 at 1:7-11.) However, the specifications of these three patents were never amended to properly reference the Big Book's issued patent number, as required by the Patent Office. See In re De Seversky, 474 F.2d 671 (C.C.P.A. 1973); Manual of Patent Examining Procedure § 608.01(p). This failure means that the Big Book is not part of the "specifications" of these three patents. Nonetheless, the Big Book remains intrinsic evidence for the '683 Patent (as it is in that patent's prosecution history) and extrinsic evidence for the others.

2. Restriction Requirements and Divisional Patent Applications

InterTrust argues that a Patent Office restriction requirement "conclusively rebuts"

Microsoft's position that the Big Book is drawn to a comprehensive VDE "invention." InterTrust's argument misses the mark for several reasons.

First, the claim construction point being made by Microsoft is that all of these claims necessarily invoke the required "features" of the VDE "invention," not that all claims require only those features. InterTrust's patent claims are free to recite additional features, which additional limitations may (or may not) make them separate "inventions" under Patent Office restriction practice. But, that is not the issue here.

Moreover, in entering the restriction requirement, the Patent Office did not indicate that it was construing the claims as non-VDE claims, requiring none of the required features of the disclosed "invention." Rather, the Patent Office merely grouped the original claims of the "Big Book" application into different categories that were supposedly "related as subcombinations disclosed as usable together in a single combination." (InterTrust Brief at 11 (citing September 25, 1996, Office Action at 2-3.) InterTrust admits in its opening brief that Rambus Inc. v. Infineon Techs., 318 F.3d 1081 (Fed. Cir. 2003), is distinguishable because none of the restriction requirements here specifically involved the VDE limitations, whereas in Rambus the limitation at issue was directly involved in the restriction requirement. (InterTrust Br. at 13, n. 7).

Also, that a restriction requirement was made does not mean that subsequent claims are directed to separate inventions. Rather, a court must closely scrutinize the scope of claims issuing from a divisional application. Gerber Garment Tech., Inc. v. Lectra Sys., 916 F.2d 683, 688 (Fed. Cir. 1990) (invalidating divisional claims for double patenting, because applicant had amended such that they were no longer distinct inventions). Here, as in Gerber, the claims at issue were changed from the original application claims that "spun off" after the restriction requirement. (Alexander Decl., ¶¶ 17.) Consequently, any "presumption" that these issued claims are directed to a different "invention" should not apply.

Finally, courts have limited claims based on descriptions in the specification, despite the fact that a patent issued from a "divisional" application. See Ballard, 268 F.3d at 1360-62 (Fed. Cir. 2001) (limiting claims of both a patent issued from the parent application and a patent issued from a divisional of such parent to exclude a particular type of valve based on statements made in common specification text and prosecution history of the parent application).

3. Claim Terms Are Construed Consistently in Related Patents

InterTrust incorrectly asserts that "divisional" patents should be separated from their parent. On the contrary, related patents should be construed consistently. Specifically, terms in patent families should generally be afforded the same construction. See AbTox, Inc. v. Exitron Corp., 131 F. 3d 1009, 1001 (Fed. Cir. 1997), amending on reh'g 122 F.3d 1019 (Fed. Cir. 1997) ("Although these claims have since issued in separate patents, it would be improper to construe this term differently in one patent than another, given their common ancestry.") Also, limitations set forth in one patent's specification or prosecution history, may act as a limitation on the related patents. Elkay Mfg. Co. v. Ebco Mfg. Co., 192 F.3d 973, 980 (Fed. Cir. 1999) ("When multiple patents derive from the same initial application, the prosecution history regarding a claim limitation in any patent that has issued applies with equal force to subsequently issued patents that contain the same claim limitation"); see also Mark I Mktg. Corp. v. R.R. Donnelley & Sons Co., 66 F.3d 285, 291 (Fed. Cir. 1995) (restricting claim scope based on prosecution of "grandparent" application).

VI. EACH OF THE TWELVE CLAIMS SHOULD BE CONSTRUED TO REQUIRE THE DISCLOSED "INVENTION"

A. '193, Claims 1, 11, 15, 19

The '193 Patent publishes the Big Book specification without any substantive additions (and thus is cited throughout this Brief as a surrogate for the Big Book).

Contrary to InterTrust's position (InterTrust Br. at 8:9-10), all four '193 Patent mini-Markman claims concern the distribution and protection of digital content, and contemplate multiple nodes and participants. Information is received (possibly from multiple upstream content providers), then stored on a device having unspecified authorized and unauthorized users, and then conditionally transferred to another device having unspecified users. The claims promise to control three forms of unauthorized use of this distributed content: copying, distributing (to the second device), and storing (on the first and/or second device):

> "if said copy control allows at least a portion of said digital file to be copied and stored on a second device...." ('193 321:10-11)
>
> "determining" or "determine" "whether said digital file may be copied and stored on a second device ...." ('193 321:7-9)

This claim language (e.g., "if ... allows," "determining whether") is not qualified. It implies that if the copying and storing are not allowed, then they are prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made to take the unauthorized action. In other words, these claims imply that their "controls" are effective in the face of the attacks identified in the Big Book.

These claimed protections against misuse cannot be achieved by encrypting the content. Encryption would not prevent the content from being accessed, copied, distributed, or stored. For these types of protection, "access control" is necessary. More particularly, the Big Book describes only the complete "invention" as providing such protection against the threats identified in the Big Book. In other words, by promising the type of effective access control protection said to be provided only by the complete VDE, these claims invoke that "invention." Their use of the vague, VDE term "control" also invokes the "invention."

B. '683, Claim 2

The '683 Patent is a "continuation-in-part" (CIP) which does not contain the Big Book's text. Although it purports to incorporate the Big Book, it fails the Patent Office's rules for incorporating "essential matter." (See supra, V. B.1 at 14.) Nevertheless, the Big Book is part of this patent's prosecution history, and thus is intrinsic evidence for claim construction purposes.

This claim also concerns a multi-node distribution system. Here, "secure containers" and "secure container rules" are distributed amongst various nodes. The claim appears to promise the ability to prevent access to or use of protected information, using the secure containers, secure container rules, and a "protected processing environment." (See Second Mitchell Decl. at 6-7.) These protections are not qualified as to the nature or severity of the threat being faced; they impliedly are effective against all threats identified in the patent or Big Book. The only system described in the Big Book or '683 Patent said to accomplish such protections, is the complete

VDE. This claim further invokes VDE by using VDE and vague terminology, such as "secure container" and "protected processing environment."

C. '721, Claims 1, 34

The '721 Patent neither contains the Big Book, nor incorporates it in the manner required by the Patent Office for incorporating essential matter into a patent. Moreover, the Big Book is not in the '721 Patent's Patent Office prosecution history. Thus, the Big Book is merely extrinsic evidence for purposes of construing these claims.

The '721 Patent purports to improve the Big Book VDE by preventing the use of executable code (specifically, "load modules" in Claim 1) except as authorized. Such prevention requires an access control capability. Claims 1 and 34 promise such protections without any qualification that they are effective only sometimes, or in some situations. Neither the Big Book nor the '721 Patent describes anything other than a full VDE system for achieving these types of promised results in the face of the threats identified in those documents. These claims further invoke the "invention" by reciting several terms that invoke VDE for context, including "protected processing environment," "tamper resistant barrier," and "security."

D. '861, Claim 58

The Big Book also is merely extrinsic evidence for purposes of construing this claim.

This patent discusses a possible attack on the "security" of "secure containers." It requires that the process of creating VDE secure containers be itself protected. ('861 4:51-64)

Claim 58 recites such a method for creating secure containers. It appears to promise the ability to prevent any access to or use of certain information (by putting the information in a secure container), except as authorized by a rule. It also provides a particular rule designed to control at least one aspect of allowed use or access. Again, the promised protection is not qualified by type or severity of threat. Neither this patent nor the Big Book describes any non-VDE system for achieving this promised capability. This claim further invokes VDE by reciting various vague and VDE terms, including "secure container" and "control."

E. '891, Claim 1

This patent publishes the Big Book without addition.

This claim appears to make the unqualified promise that it prevents an appliance from using content protected by controls received from two remote entities, except as authorized by those controls. This ability to prevent all use implies an ability to control access. Again, the patents describe no non-VDE system having this capability. This claim also uses several vague and VDE terms, such as "secure operating environment," "securely receiving," "control," "securely processing," and "securely applying."

F. '900, Claim 155

This patent repeats the Big Book, but also adds to it. It addresses various possible attacks against VDE's protections, including one in which a VDE's foundation software (which, e.g., runs to create a VDE "host processing environment") is copied onto another machine to form a rogue VDE node. ('900 233:8-15). One of the solutions described in this patent is to embed a unique identifier, called a "machine signature," into the VDE software so that it cannot run on a different machine. ('900 237:40-54, 239:5-14).

Claim 155 recites a method using "machine check programming" for checking a VDE host processing environment and halting processing. This method also is unqualified, i.e., it does not rule out any of the types or severities of threat described in this patent. Also, it uses several VDE specific or otherwise vague terms, such as "virtual distribution environment," "host processing environment," "machine check programming," and "tamper resistant software," which need to be clarified and construed in light of the VDE "invention."

G. '912, Claims 8, 35

This patent is a "divisional" patent which publishes the Big Book without change.

These claims are somewhat similar to those of the '721 Patent. Claim 8 appears to promise the ability to prevent use of a load module within an execution space, except as authorized. Claim 35 appears to promise the unqualified ability to prevent use of certain "specified information," in part by protecting the process of creating the "component assembly" which controls that use. By preventing unauthorized uses, each claim implies an access control capability. Again, the Big Book describes no non-VDE system with this unqualified capability. These claims also use several VDE or vague terms, such as "component assembly," "load module," "level of security," "securely assembling," and "secure container."

In sum, had these twelve claims used only precise, well-defined, non-VDE terminology, and not promised the types and levels of protection provided by VDE, then they might not have invoked the disclosed "invention." That, however, is not the case.

VII. CONSTRUCTION OF THE CLAIM TERM "USE"

Central Dispute: Whether an encrypted file may be "used" without decrypting it.

As explained above, VDE prevents all forms of unauthorized "use" of protected information, including forms of misuse which do not require decryption, such as deleting or altering someone else's encrypted content.

Ordinary Meaning: Microsoft's construction follows from the ordinary, everyday meaning of "use." A "use," of course, may be a "misuse." In "security" systems, the most important uses to address are the potential misuses, including those by unauthorized users. Microsoft's construction does that, and includes several uses which may be misuses (such as deleting someone else's data).

Microsoft's Construction: "(1) To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.)...." (JCCS Exh. A at Row 42).

This is precisely how the term "use" is used in the Big Book and '683 Patent:

> "These appliances typically include a secure subsystem that can enable control of **content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc.**" ('193 9:24-27)
>
> "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that **the moving, accessing, modifying, or otherwise using of information** can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-31)
>
> "Provides non-repudiation of use and may record specific **forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.**" ('683 6:46-48)

(Alexander Dec. Exh. D at 23(G), 23(C), 23(A).) Nothing in these patents counters these Big

Book definitions of "use" as including copying, encrypting, saving, modifying, and moving.

Importantly, many of these actions which the Big Book refers to as "uses" cannot be blocked by encryption and, conversely, require no decryption of the content to perform. That such uses are indeed "uses," is further confirmed by the parties' agreed definition of "tampering" (which includes "altering" within "use" (see JCCS Exh. I at Row 8)), and InterTrust's proposed definition of "VDE" (which includes "distribution" within "use" (see JCCS Exh. A at Row 86)).

Microsoft's proposed construction further requires that "(2) In VDE, information Use is Allowed only through execution of the applicable VDE Control(s) and satisfaction of all requirements imposed by such execution." (See JCCS Exh. A at Row 42). This is VDE's "prevent unauthorized use" protection mechanism, governed by VDE controls, which is found throughout the Big Book, and explained by Prof. Maier (Maier Decl. at 7-8, 38-41).

InterTrust's Proposed Construction: InterTrust's proposed construction of "use" is typical of most of its constructions: short, unclear, and contrary to the Big Book: "to put into service or apply for a purpose, to employ." (See JCCS Exh. A at Row 42). This loose language may be fine as a general concept, but is not adequate for a claim construction. It does not clearly or precisely define the types of use (e.g., misuses) of digital information it encompasses or excludes. On the contrary, it would leave the jury and public guessing about which of the following actions, **expressly identified as "uses" in the patents**, are "uses": copying, encrypting, saving, modifying, and moving.

InterTrust apparently contends that nothing is a "use" of information if it cannot be prevented by encryption alone. In other words, if content is encrypted, a "use" of that information must require decryption, or else it is not a "use." Per InterTrust, apparently, none of these Big Book uses, is a use: deleting content, altering it, saving it, encrypting it, copying it, or moving it.

This position is contrary to the Big Book's above-quoted express statements that "use" includes deleting, saving, encrypting, moving, and copying. More importantly, it is contrary to the core promise of the VDE "present invention" that its access control capabilities can prevent all unauthorized access to and use of protected content, not just those uses which could be blocked through encryption.

The Court should expressly include within "use" all of those actions expressly identified as "uses" in the Big Book and the '683 Patent, as set forth in Microsoft's construction.

VIII. CONSTRUCTION OF THE CLAIM TERM "COPY"

Central Dispute: Whether a reproduction is still a "copy" if it is unusable or inaccessible to someone.

Ordinary Meaning: Under its ordinary meaning, to "copy" something is to reproduce it, and the resulting reproduction is a "copy." The copy, of course, remains a copy even if it is locked away and inaccessible. It also remains a copy if given to someone who cannot use it.

Microsoft's Construction: "(1) To reproduce all of a Digital File or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. (2) Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. (3) **The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible.**" (See JCCS Exh. A at Row 5).

This is how the Big Book uses the term "copy." A copy of an encrypted electronic file is still a copy even when possessed by someone who has no right to decrypt it or otherwise use it. Thus, the Big Book refers to a reproduction of a video program as a "copy" even though its recipient cannot watch or copy it: "Even if a consumer has a **copy of a video program**, she cannot watch or copy the program unless she has "rules and controls" that authorize use of the program." ('193 53:60-62). On the other hand, when the Big Book means a copy which is usable, it says so: "For example, if a software program was distributed as a traveling object, a user of the program who wished to supply it or a **usable copy** of it to a friend would normally be free to do so." ('193 131:65-132:1). (Alexander Dec. Exh D at 10(C)-10(E).)

InterTrust's expert, Prof. Reiter, has testified that this everyday "reproduction" sense of the word "copy," in which a copy is still a copy even if possessed by someone who cannot decrypt it, is "a very common use of the word 'copy.'" (Reiter Depo. at 64:12-65:8, 66:1-15)). He also has conceded that the Big Book used the term "copy" in this manner in the above "video program" quote, and elsewhere. (Reiter Depo. at 68:5-70:7, 74:21-75:17).

InterTrust's Proposal: Despite this usage in the Big Book and these concessions of its expert, InterTrust nevertheless urges the Court to dismiss this "very common" usage and construe "copy" as if a copy is no longer a copy when locked away or given to someone who cannot decrypt it. Rather than expressly say so, however, InterTrust says merely that "the reproduction must be useable." (See JCCS Exh. A at Row 5). As interpreted by its expert, Prof. Reiter, InterTrust does not here mean "usable" in the VDE sense of "use" (described above). Rather, by "must be usable," InterTrust apparently means that a reproduction of encrypted content is not a copy when possessed by someone who cannot decrypt it. In other words, whereas the '193 claims expressly limit the number of "copies" which can be made, InterTrust urges the Court to read these claims as if they limit the number of "decryptable (by present holder) copies." InterTrust's proposal is unworkable, contrary to the specification's use of "copy," and wholly divorced from the core VDE "prevent unauthorized access" capability.

Unworkable: Under InterTrust's apparent theory, a non-copy would become a copy when handed to someone who can decrypt it, and then become a non-copy again when handed back. Such a vacillating status as "copy" is not workable. How can a system "control copying," if the reproduction's status as a "copy" depends on who happens to possess it in the future?

Contrary to Specification: The Big Book not once suggests that a "copy" **must** be decryptable or "usable." On the contrary, as noted above, the Big Book focuses on ways to **prevent** use (e.g., misuse) of files and copies; expressly states that one needs appropriate controls to use a "copy" ('193 53:60-63); and refers to a "usable copy" to indicate that controls allow the copy to be used ('193 131:67). Indeed, Prof. Reiter agreed that InterTrust's proposed construction of "copy" was inconsistent with the above-quoted Big Book's use of the term "copy" in connection with a video program. (Reiter Depo. at 71:19-73:17).

Contrary to the VDE "No Unauthorized Access" Promise: Perhaps most importantly, in its construction of "copy," InterTrust again ignores and contradicts the VDE "present invention."

These claims concern copying not only by authorized end-users, but also by unauthorized mis-users. Preventing such unauthorized copying, even by someone who is unable to decrypt those copies, is an important "security" feature. For example, unauthorized copying of encrypted files can be used as a "denial of service attack" on a computer system by replicating the encrypted files into a computer's memory to deny legitimate access to that memory by authorized users. (This attack is especially effective if the files are written to a write-only medium.) Or, an attacker could copy multiple encrypted files to his own computer to study the encryption scheme. In neither of these examples was the attacker authorized to decrypt the encrypted "copy," but he nevertheless was able to use copying of encrypted files for his own unauthorized purposes. (See Second Mitchell Decl. at 6-7 (discussing "copy").)

The claimed methods can block all unauthorized copying because VDE supposedly is able to block all access to the encrypted content. InterTrust's position wrongly assumes that only the ability to decrypt content is being controlled. In other words, by arguing that a "copy" is not usable if it cannot be decrypted (and thus is not a copy), InterTrust is trying to transform this claim which prevents all unauthorized copying (i.e., has at least two levels of protection), into a claim which merely prevents unauthorized decryption of copies (i.e., has only one level of protection).

<u>Other Disputes Over This Term</u>: One, of course, may copy all of something or only a portion. InterTrust argues that copying a portion of a file can be referred to as copying the file, while Microsoft submits that copying a portion is just that, copying a portion. If a claim speaks of copying a file, it means copying the entire file. When the claims, and patents, mean to refer to a portion, they say "portion." (Compare '193, Claim 1 ("copying at least a portion of said digital file"), with '193 Claim 11 ("determining whether said digital file may be copied."))

InterTrust also argues that "copying" includes altering something, "as long as the essential nature of the content remains unchanged." (See JCCS Exh. A at Row 5). That is unsupported by the patents, and unworkably vague.

IX. CONSTRUCTION OF "SECURE"; "SECURELY"

Central Dispute: Whether a "secure" condition is one in which the threats identified in the patents are prevented, rather than one in which, e.g., some form of attack is detected (but not prevented).

Ordinary Meaning: It is well recognized in computer science that "secure" is a label for an achieved condition or state of being:

> "**State achieved** by hardware, software or data as **a result of successful efforts** to prevent damage, theft or corruption," (Spencer, 156; see Reiter Depo.at 221:4-7) (cited by InterTrust for another term)
>
> "Security is a negative attribute. **We judge a system to be secure if we have not been able to design a method of misusing it** which gives some advantage to the attacker." (Davies, p. 4)
>
> "Definition 4-1. A *security policy* is a statement that partitions the states of the system into a set of *authorized*, or *secure*, states and a set of *unauthorized*, or *nonsecure*, states . . . Definition 4-2 A ***secure system* is a system that starts in an authorized state and cannot enter an unauthorized state.**" (Italics in original) (Bishop, p. 95)

(Alexander Dec. Exh. D at 19(JJ), 19(XX), 19(TT).) (See also Reiter Depo. at 30:11-34:5, 35:9-36:18, 222:11-223:1.)

As explained in Prof. Mitchell's first Declaration, there are myriad flavors and degrees of being "secure," depending on a host of contextual variables, such as what is being protected, against what, for how long, to what degree, etc. The patents confirm this by using "secure" to mean different things in different places. The unanswerable question is what does "secure" mean in these context-light claims? (See Microsoft's Motion for Summary Judgment on Indefiniteness).

InterTrust's Proposed Construction: InterTrust's proposed construction of "secure" is so extreme that we address it first: "One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that Access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose." (See JCCS Exh. A at Row 3).

"One or more mechanisms are employed ....": InterTrust's construction is contrary to the ordinary meaning of "secure" in many respects. First, being "secure" is like being "intelligent" or "beautiful;" it is a condition or a state of being. It is not a statement that some effort was made to become secure (or intelligent or beautiful); it is a label confirming a successful result. For example, placing a combination lock on a safe "employs" a security "mechanism," but that does not mean that the safe is "secure" (e.g., the combination might be easy to guess, or even posted on the safe; the safe's door might be left unlocked, or the safe's walls might easily be broken, etc.).

InterTrust's proposed construction is wrong in this very basic respect. It says that something is "secure" if some effort is made: the result doesn't matter. That is illogical, contrary to the ordinary meaning, and contrary to the Big Book's promises that VDE's security mechanisms can achieve a truly secure environment.

"To prevent, detect, or discourage ....": This is another example of how far InterTrust is willing to distance the claims from the VDE "present invention." Whereas the VDE invention promises the ability to **prevent** all access, use, observation, and interference with protected content, InterTrust would have the Court rule that something is "secure" even if its content is easily destroyed, copied, distributed, and read by others, so long as the system "detects" or "discourages" this misuse. Detecting misuse can be an important function that helps achieve a secure condition, but detecting alone, without preventing misuse, is not security.

Indeed, that InterTrust would urge that a "secure" container, environment, space, memory, etc., may not prevent (or even discourage) any threat whatsoever, no matter how weak the attack, illustrates how flawed its whole approach to claim construction has been. Claim construction is not a word game where one hunts for bits and pieces of definitions from dictionaries written without the "invention" in mind, and tries to fit them together to get the broadest and vaguest possible meaning of a claim term. Rather, as the Patent Statutes require, the Supreme Court has held, and the Federal Circuit has recognized, "what is claimed by the patent application must be the same as what is disclosed in the specification."

"Such mechanisms may include concealment, Tamper Resistance, Authentication and access control.": Prof. Reiter has testified that, under InterTrust's proposal, the term "secure" **does not require any** of these listed forms of protection. (Reiter Depo. at 201:14-204:14). This, again, is at odds with the Big Book's promise that VDE prevents all unauthorized access, use, observation, and interference.

"Security is not absolute, but is designed to be sufficient for a particular purpose": This statement points out a basic problem with the use of "secure" in these claims and with InterTrust's proposed construction. As with "intelligence," being "secure" is a multi-dimensional, subjective characteristic for which some objective criteria is necessary if skilled evaluators are to objectively determine whether or not something is "secure." That the term "secure" is used in the specification to refer to different things in different contexts, as InterTrust notes, only confirms why context is all important to an understanding of what the term means in the claims. Neither these claims, nor InterTrust's "sufficient for a particular purpose" proposal, however, provides such context or any objective criteria for evaluating what is or is not "secure."

The "designed to be" language of InterTrust's proposed definition language hints that, in InterTrust's view, the "purpose" necessary for evaluating whether something is secure can be gleaned not from the patents, but from the "designer" of an individual accused system or components. That makes no sense. Assume that A and B design two identical systems, each with a different "purpose" in their designs. C acquires these identical systems and offers them to a potential customer D who first wants to know whether these two identical systems are "secure" as meant in these patent claims. It simply cannot be true that one system is "secure" while the other identical system is not (because of the different purposes of their designers). Rather, the necessary context, purpose, and objective criteria for evaluating whether any given system is "secure" as meant by these claims (if it can be discerned at all), must be fixed within the patents themselves.

Microsoft's Construction: Unlike InterTrust's proposal, Microsoft's construction of "secure" is workable, precise, and honors the basic premise of VDE. Specifically, to the extent a construction is forced onto this indefinite claim term, it should be that the term "secure" indicates that each type of property identified in the patents is "truly secure" against all types and levels of threats identified in the patents. In part, this means that "secure" is "(1) A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto." (See JCCS Exh. A at Row 3).

This is not a standard definition of "secure." Nor is it an express definition from the Big Book (which doesn't offer one). But, if the Court denies Microsoft's indefiniteness motion, and finds the term "secure" sufficiently clear to construe, this is the fairest approach to that construction. Specifically, this "true security" construction follows from InterTrust's assertion that "security is designed to be sufficient for a particular purpose." Here, the Big Book describes a wide range of possible security threats, including strong and sophisticated attacks against valuable information where only this proposed "true security" would be acceptable. None of the patent claims excludes such high-value, strong-attack situations. On the contrary, they apparently maintain a secure state in the face of all attacks mentioned in the patents. Therefore, the fairest construction is the one that makes sense over the whole range of disclosed attack situations, namely "true security" where all properties are protected against all attacks identified in the Big Book.

X. CONSTRUCTION OF "SECURE CONTAINER"

Central Dispute: Whether a "secure container" must prevent unauthorized access to its contents.

A VDE secure container is one of the core VDE components that provide the capabilities touted in the Summary of the Invention.

Ordinary Meaning: The parties agree that the term "secure container" has no ordinary meaning in this field. (See, e.g., Reiter Depo. at 275:6-276:10.)

Microsoft's Construction: (1) A VDE Secure Container is a self-contained, self-protecting data structure which ... (b) cryptographically protects that information from all unauthorized Access and Use, ... (d) permits the association of itself or its contents with Controls and control information governing (Controlling) Access to and Use thereof, and (e) prevents such Use or Access (as opposed to merely preventing decryption) until it is "opened." (See JCCS Exh. A at Row 57).

As used in the Big Book, a VDE "secure container" protects content it contains by preventing all access to and use of that content except as authorized by VDE via satisfactory execution of VDE controls associated with the secure container. In effect, a VDE secure container hides the content from users while VDE "controls" act as guards that escort authorized users to that content and supervise their use of it. (Alexander Dec. Exh. D at 20(A)-20(C), 20(E)-20(G).)

The Big Book describes details of only one embodiment of a secure container. In that embodiment, the secure container (in conjunction with the rest of VDE) blocks all direct access to its contents, and requires satisfaction of several controls, including one created by an ACCESS method[5]:

> "Even if the object is stored locally to the VDE node, **it may be stored as a secure or protected object[6] so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object.**" ('193 192:14-19)

A secure container, then, is part of the second layer of protection discussed above. As noted in the below quote, not only is the content "encrypted" (first layer of protection) but so is the "content source and routing information" (second layer).

> "ACCESS method 2000 reads the ACCESS method MDE from the secure database, reads it in accordance with the ACCESS method DTD, and **loads encrypted content source and routing information** based on the MDE (blocks 2010, 2012). **This source and routing information specifies the location of the encrypted content.** ACCESS method 2000 then determines whether a connection to the content is available (decision block 2014). ('193 192:36-52)

[5] InterTrust construes "access" as meaning "To obtain something so it can be used," which is true, although incomplete.

[6] This sentence refers to a "secure object." In VDE, a "container" and its contents "can be called an 'object.'" ('193 58:43-44).

Prof. Maier explains this VDE "secure container" mechanism at greater length. (See also Reiter Depo. at 117:18-23; 125:20-126:4; '683 Patent 15:67-16:4. Maier Decl. at 38-41.)

This "access control" ability of VDE secure containers is critical to VDE's promise to content owners that it can prevent (not simply detect) all access to and use (not just decryption-based uses) of protected content. Without this access control ability of VDE generally, and secure containers in particular, VDE's promised ability to control, govern, audit, etc. all accesses and uses, would be a lie.

InterTrust's Proposed Construction: InterTrust's proposed construction of "secure container" is a far cry from the VDE "secure container": "A Container that is Secure." (See JCCS Exh. A at Row 57). As this is interpreted by Prof. Reiter, merely detecting a single form of misuse of some of its contents, would make a container a "secure container," even if the container could not prevent **any** unwanted access, misuse or interference with the contents. That certainly does not sound "secure," and, more importantly, makes no sense in light of the Big Book's and other InterTrust patents' proclamations of the abilities of a VDE secure container:

> "**Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility.**" ('683 8:50-52).
>
> "Even if the object is stored locally to the VDE node, **it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object.** ('193 188:59-67).

XI. CONSTRUCTION OF "TAMPER RESISTANT BARRIER"

Central Dispute: Whether a "tamper resistant barrier" must be a physical device, and prevent unauthorized access, observation, and interference.

Another of the required VDE mechanisms for providing the promised VDE capabilities, is a VDE secure processing environment, formed by a hardware-based tamper resistant barrier.

Ordinary Meaning: The ordinary meaning of "tamper resistant barrier" denotes a physical device. More specifically, the term "tamper resistant barrier" would have been understood in 1995 in reference to cryptographic coprocessors such as smart cards. (See Reiter Depo. at 137:15 – 138:17).

Microsoft Construction: "(1) An active device that encapsulates and separates a Protected Processing Environment from the rest of the world. (2) It prevents information and processes within the Protected Processing Environment from being observed, interfered with, and leaving except under appropriate conditions ensuring security. (3) It also Controls external access to the encapsulated Secure resources, processes and information. (4) A Tamper Resistant Barrier is capable of destroying protected information in response to Tampering attempts." (See JCCS Exh. A at Row 71).

To properly construe this term requires consideration of another "access control" promise of VDE.

As noted above, VDE concerns both security **and** commerce. Hence, it does not just prevent unauthorized access to protected content, it also allows and governs authorized access to, and use of, that content. That, however, presents a possible security hole. The processes used to allow and govern authorized access or use might be observed by attackers and altered to permit improper access to and use of protected content. Therefore, as a corollary to its promise to prevent protected **content** from any unauthorized access, VDE also promises that it is capable of preventing (not merely detecting) all unauthorized observation of and interference with the VDE processes which govern such access and use.[7]

> "SPU 500 is enclosed within and protected by a '**tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions.**" ('193 59:48-53)
>
> "SPU 500 provides a tamper-resistant protected processing environment ("PPE") in which processes and transactions can take place securely and in a trusted fashion." ('683 16:60-62)

Prof. Reiter has agreed that the Big Book describes mechanisms to prevent all types of tampering (unauthorized interference) with VDE processes. (Reiter Depo. at 55:17-60:1).

[7] Whether users can choose not to use all of a system's capabilities does not change the fact that those capabilities allegedly exist.

This corollary promise—the ability to prevent VDE processes from unauthorized observation and interference—informs the proper construction of "tamper resistant barrier." As described in the first above quote, a tamper resistant barrier encapsulates a special-purpose "Secure Processing Unit" (SPU). This physical tamper resistant barrier prevents both information and processes within the Protected Processing Environment from being "observed, interfered with, and leaving" except under appropriate conditions ensuring security.

> "SPU 500 in this example is an integrated circuit ("IC") "chip" 504 including "hardware" 506 and "firmware" 508. ... "Hardware" 506 also contains long-term and short-term memories to store information securely so **it can't be tampered with.**" ('193 59:60-60:3)

> "BIU 530 is **designed to prevent unauthorized access to internal components within SPU 500 and their contents**. It does this by only allowing signals associated with an SPU 500 to be processed by control programs running on microprocessor 520 and not supporting direct access to the internal elements of an SPU 500." ('193 69:6-11)

As InterTrust notes, the Big Book also refers to a "tamper resistant barrier" which is not a physical, hardware device. However, the "tamper resistant barrier" in the mini-Markman claims is properly construed as the hardware variant, for three reasons.

First, the Big Book promises "true" security. It promises the ability to "prevent" unauthorized uses, etc., and "ensure" that rights will be enforced, and "guarantee" trustworthiness, even when faced with strong, sophisticated attacks against high-value content. Nothing in the claims indicates an inability to live up to these promises and protect such high-value content against such strong attacks. Only the hardware-based tamper resistant barrier is described as providing that sort of true protection for the most valuable content in even high-risk surroundings.

> "HPEs 655 may (as shown in FIG. 10) be provided with a software- based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a 'secure' HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. **The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional secure (albeit possibly less secure than the SPE) processing** using host processor or other general purpose resources that may be available within an

> electronic appliance 600. Any service may be provided by such a secure HPE 655" (‘193 80:22-36)
>
> "**No software-only tamper resistant barrier 674 can be wholly effective against all of these threats. A sufficiently powerful dynamic analysis (such as one employing an in-circuit emulator) can lay bare all of the software-based PPE 650's secrets.** Nonetheless, various techniques described below in connection with FIG. 69A and following make such an analysis extremely frustrating and time consuming--increasing the 'work factor' to a point where it may become commercially unfeasible to attempt to 'crack' a software-based tamper resistant barrier 674." ('900 233:24-33)

Second, if these claim terms were construed to cover the software variants, they would be much too vague. There would be no objective measure for distinguishing between a barrier which is tamper resistant and one which is not tamper resistant.

Third, the Big Book states that a Secure Processing Unit (with its physical tamper resistant barrier) is necessary wherever protected content is assigned usage related control information, or used. As all of the mini-Markman claims contemplate one or both of these two conditions, each claim necessarily requires a hardware tamper resistant barrier.

> "VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. **VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a 'virtual black box,' a collection of distributed, very secure VDE related hardware instances** that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means." ('193 15:14-27)
>
> "**Summary of Some Important Features Provided by VDE in Accordance With the Present Invention** ... VDE employs **special purpose hardware** distributed throughout **some or all locations** of a VDE implementation: a) **said hardware controlling important elements of**: content preparation (such as causing such content to be placed in a VDE content container and associating content control information with said content), content **and/or** electronic appliance usage auditing, content usage analysis, **as well as content usage control**; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors" ('193 21:43-45; 22:20-31)
>
> "**A hardware SPU (rather than a software emulation) within a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required.**" ('193 49:15-17)

> "**Physical facility and user identity authentication security procedures** may be used **instead of hardware SPUs at certain nodes**, such as at an established financial clearinghouse, **where such procedures may provide sufficient security** for trusted interoperability with a VDE arrangement employing hardware SPUs at user nodes." ('193 45:60-65)

(See also Maier Decl. at 9-11.)

InterTrust's Proposed Construction: "Hardware and/or software that provides Tamper Resistance." InterTrust defines "Tamper Resistance" as "Making tampering more difficult and/or allowing detection of tampering." (See JCCS Exh. A at Row 67).

This proposal raises more questions than it answers. For example, "making tampering more difficult" than what? What does "allowing detection of tampering" mean? Not preventing detection? Are the walls of straw house a tamper resistant barrier because they allow detection of a fire? And, as usual, InterTrust's proposed construction is contrary to VDE. The "invention" did not settle for mere detection; it was touted as preventing all unauthorized access, use, observation, and interference. InterTrust may regret those promises but it cannot erase them.

XII. CONSTRUCTION OF "PROTECTED PROCESSING ENVIRONMENT"

Central Dispute: Whether a "protected processing environment" must have a physical "tamper resistant barrier" and prevent unauthorized access, observation, and interference.

This claim term presents the same key issue as "tamper resistant barrier."

Ordinary Meaning: The parties agree that there is no ordinary meaning of "protected processing environment."

Microsoft Construction: "(1) A uniquely identifiable, self-contained computing base trusted by all VDE nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be Accessed and Used only as expressly authorized by VDE Controls. (2) At most VDE nodes, the Protected Processing Environment is a Secure Processing Environment . . . (3) The Tamper Resistant Barrier prevents all unauthorized (intentional or accidental) interference, removal, observation, and use of the information and processes within it, by all parties (including all users of the device in which the Protected Processing Environment resides), except as expressly authorized by VDE Controls." (See JCCS Exh. A at Row 62).

As InterTrust notes, the Big Book describes two categories of processing environment. One, called a Secure Processing Environment (SPE), is hardware-based, centered on the Secure Processing Unit (SPU) with a hardware tamper resistant barrier. This SPE is said to provide "true" security. Another, called a Host Processing Environment (HPE), lacks an SPU, and if it has any tamper resistant barrier, it is software based. The Big Book says that an HPE provides less protection and may not be "truly secure." The patent uses the term "Protected Processing Environment" to refer to either an SPE, or HPE, except as otherwise indicated. And, it says that an HPE may be "secure" or "non-secure." (Alexander Dec. Exh. D at 16(C), 16(H), 16(I), 18(A)-18(E).)

The same three reasons cited above for "tamper resistant barrier" also demonstrate that these claims' "protected processing environment" must be the hardware-based Secure Processing Environment, not the software-based Host Processing Environment.

InterTrust's Proposed Construction: (1): "An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat . . . ." (See JCCS Exh. A at Row 62).

This definition is vague in several respects. For example, what does it mean to "at least in part protect" processing and/or data? What exactly does the "in part" modify? Does protection mean prevention, or is merely allowing detection good enough as InterTrust suggests for "secure"? And, as the level of protection depends on the threat, what precise threat(s) are assumed by this claim term, and what "level of protection" is required by those threats? And, is the "processing and/or data" inside the environment being protected from the outside world, or is the outside world being protected from what's inside the environment? In any event, InterTrust's proposal again fails to honor any of the requirements of the VDE "invention," including its ability to prevent all unauthorized access, use, observation, and interference.

XIII. CONSTRUCTION OF "COMPONENT ASSEMBLY"

Central Dispute: Whether a "component assembly" is executable.

In the disclosed "invention," "component assemblies" are dynamically created executable components (called VDE's "basic functional unit") which help give VDE its touted flexibility and user-configurability.

Ordinary Meaning: The parties agree that the term "component assembly" has no ordinary meaning in this art.

Microsoft's Construction: "(1) A cohesive Executable component created by a channel which binds or links together two or more independently deliverable Load Modules ..., and associated data; ...." (See JCCS Exh. A at Row 99).

In the Big Book, the term "component assembly" (also called "component") uniformly is used to refer to executable components, which are an assembly of independent, executable load modules and data. These VDE component assemblies may be transferred between VDE nodes to perform various tasks, and each is "executable." (See Alexander Dec. Exh. D at 24-4(CC), 6(B, C).) The **only** kind of "component assembly" mentioned in these patents is this VDE component assembly.

InterTrust's Proposed Construction: "Components are code and/or data elements that are independently deliverable...." There is no support for this notion that a component assembly may be mere non-executable data. None of the above-quotes (e.g., "component assemblies 690 are the basic functional unit") would make any sense if the component assembly were not executable. Indeed, as noted below, the most important executable component in VDE—the VDE control—is a component assembly.

XIV. CONSTRUCTION OF "CONTROL" (NOUN)

Central Dispute: Whether a "control" is an executable component.

Satisfactory execution of "VDE controls" give authorized users access to content protected by VDE secure containers and VDE protected processing environments.

Ordinary Meaning: While the term "control" is used frequently in computer science, it does not have any precise ordinary meaning, but rather means different things in different contexts.

Microsoft's Construction: "(1) Independent, special-purpose, Executable, which can execute only within a Secure Processing Environment. (2) Each VDE Control is a Component Assembly dedicated to a particular activity (e.g., editing, modifying another Control, a user-defined action, etc.), particular user(s), and particular protected information, and whose satisfactory execution is necessary to Allowing … that activity…." (See JCCS Exh. A at Row 4).

VDE "controls" can be explained, partially, with an analogy to a rare books library holding valuable texts. Each different type of access and use of these texts is controlled by a different set of rules, and possibly a different guard or librarian. One guard checks one list of permitted visitors to enter the library; another may check a shorter list for entry to a particular room with particularly valuable texts; another librarian will follow other rules to collect certain texts and supervise their viewing; another may follow other rules to determine whether the visitor may copy any portion of the text; and another may need to authorize or stay after hours to translate (decrypt) the text, or perhaps only particular pages thereof. In VDE, these separate guards and librarians are independent, executable VDE controls which, based on applicable rules, allow a particular type of access or use, and then monitor that access or use. Prof. Maier's explanation of VDE explains an example of these independent VDE controls in operation.

The Big Book states that an important feature of VDE is that each VDE control specializes in allowing and supervising only one type of access or use. VDE controls independently govern separate activities (e.g., access or copy or read); independently govern arbitrarily small portions of data; and are configurable by all participants (subject only to other participants' controls).

> "**Secure electronic controls** can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be 'destroyed' after a certain elapse of time or real time or after a certain number of

> handlings, etc.) **Persistent secure electronic controls** can continue to supervise item workflow even after it has been received and 'read.'" ('683 6:18 - 9:4)

InterTrust's Proposed Construction: InterTrust's proposed construction of "Control" again ignores the Big Book in favor of a vague, non-VDE construction: "Information and/or programming Governing operations on or use of Resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations." (See JCCS Exh. A at Row 4). With its "information and/or programming" language, InterTrust suggests that a "control" may be mere non-executable information. More specifically, InterTrust has equated non-executable "rules" and executable "controls." This confuses the guard (control) with the rules he or she follows in allowing and monitoring certain accesses or uses. In the Big Book's usage, a "rule" need not be executable, but a "control" must be.

InterTrust argues that "rules and controls" are equated with "control information," and control information may be mere data, and therefore a control may be mere data. But, under that "logic," apples may be oranges because a sentence in a text reads "apples and oranges (fruit)." The patents do not equate rules and controls, but rather distinguish them by, e.g., often referring to "rule **and/or** control":

> "...at least one **rule and/or control** associated with the software agent that governs the agent's operation." ('193 241:2-3)
>
> "If necessary, trusted go-between 4700 may obtain and register any methods, **rules and/or controls** it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683 47:42-45)

Just as it makes no sense to refer to "apple and/or apple," it would make no sense to refer to "rule and/or control" if they were the same.

XV. <u>CONSTRUCTION OF SOME OTHER TERMS AND PHRASES</u>

<u>"A budget specifying the number of copies which can be made of said digital file"</u> (JCCS Exh. A at Row 6): InterTrust's proposed construction refers to a budget "stating the number of copies that can be made of the digital file," without specifying "can be made since when?" or "by

whom?" or "by what?" Microsoft's construction answers these open questions. (See also Reiter Depo. at 267:18-268:15.)

"Container" (JCCS Exh. A at Row 57): InterTrust proposes that a "container" "means a digital file containing linked and/or embedded items." Prof. Reiter, however, could think of no non-empty digital file which did not "contain linked and/or embedded items," and thus all digital files would qualify as "containers." That is not how this term is used in InterTrust's patents. (See Alexander Decl. Exh. D at 20(A-D).)

"Containing" (JCCS Exh. A at Row 58): The parties disagree on whether storing an indication of where an element may be found, constitutes "containing" that element. The patents are internally inconsistent on this; sometimes saying that "referencing" something is "containing" it; and other times indicating that "referencing" something is an alternative to "containing" it. (See, e.g., Alexander Decl. Exh. D at 24-8(I) ("containing or referencing").) As the normal, ordinary meaning of "contain" is to include within, not reference, the Court should adopt that meaning.

"Controlling" (JCCS Exh. A at Row 7): InterTrust's proposed construction of "control" as a verb is typically vague: "to exercise authoritative or dominating influence over; direct." This loose "influence" of the sort pertinent to persons, not computers, is not what the Big Book promises the owners of content entrusted to VDE. They were promised strict control (including monitoring) over all access and uses, including the ability to prevent (not merely detect) unauthorized access and use. (See Reiter Depo. at 165:3-9.)

Moreover, "controlling" in this "invention" is done at an arbitrary granularity, which is an important feature that the Big Book relied upon to distinguish prior art:

> **"VDE also** extends usage control information to an arbitrary granular level **(as opposed to a file based level provided by traditional operating systems)"**

(See Alexander Decl. Exh. D at 24-4(X) ('193 275:8-11)).

"Controlling the copies made of said digital file" (JCCS Exh. A at Row 7): Whereas the claim refers to "controlling the copies," InterTrust reads the claim more as "controlling the copying." Also, InterTrust's proposal suggests that the copies are transferred to the second device, but the claims recite that the file (as opposed to any copy) is transferred.

<u>"Derives information from one or more aspects of said host processing environment"</u> (JCCS Exh. A at Row 92): Prof. Reiter links this claim language to the "machine signature" technique described in the '900 Patent. That technique derives a "unique" signature of an appliance so that the HPE-forming software will not run on any other appliance. InterTrust's proposed construction lacks this "unique machine signature" technique. Under InterTrust's proposed construction, the derived information may serve no security purpose at all, which again is contrary to the patent.

<u>"Host Processing Environment"</u> (JCCS Exh. A at Row 87): The Big Book states that a "Host Processing Environment" may be secure or not secure. InterTrust's proposed construction requires security, and thus is contrary to the Big Book. Microsoft's construction explains what it means in the Big Book for a "host processing environment" to be non-secure.

<u>"Identifying (Identify)"</u> (JCCS Exh. A at Row 28): In common usage and these patents, to identify someone or something is to establish the person or thing as a particular individual or thing. InterTrust tries to expand this common understanding with its proposal: "establishing the identity of or to ascertain the origin, nature, or definitive characteristics of; ...." This is contrary to the ordinary meaning, and, again, too vague. Is gray hair a "definitive characteristic" of a person? Is a particular manufacturer of a device sufficient to establish its "nature?" The jury and public would have to guess.

<u>"Tamper Resistance"</u> (JCCS Exh. A at Row 67): InterTrust's proposed construction, "Making tampering more difficult and/or allowing detection of tampering," suffers from the same type of defects as InterTrust's other proposals. For example, "more than difficult than what?" Also, merely detecting tampering but not stopping it, plainly is not what VDE means by "tamper resistance."

For the foregoing reasons, Microsoft's proposed constructions should be adopted.

Dated: April 7, 2003

By: ______________________________
ERIC L. WESENBERG

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

DERWIN & SIEGEL, LLP
DOUGLAS K. DERWIN - #111407
3280 Alpine Road
Portola Valley, CA 94028
Telephone: (408) 855-8700
Facsimile: (408) 529-8799

INTERTRUST TECHNOLOGIES CORPORATION
JEFFERY J. McDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA **PLAINTIFF INTERTRUST TECHNOLOGIES CORPORATION'S REPLY MEMORANDUM ON CLAIM CONSTRUCTION** Date: May 12, 29, & 30, 2003 Time: 9:00 a.m.
AND COUNTER ACTION.	

TABLE OF CONTENTS

TABLE OF CONTENTS
(cont'd)

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES
(cont'd)

I. INTRODUCTION

Microsoft's claim construction positions derive from a single underlying premise: the details of the "VDE" embodiment described in the specifications must be read into every claim, and every claim element must be interpreted so as to include all of the VDE limitations. According to Microsoft, this is so because the patents "promise" an extremely high degree of security ("truly secure") that Microsoft alleges can only be supplied by the VDE embodiment.

Microsoft acknowledges, however, that the patents describe varying levels of security, ranging from the extremely high degree of security provided by the "truly secure" embodiment to much lower levels of security. The patents refer to all of these levels of security as "secure," and each of them represents a degree of security appropriate to particular circumstances. Microsoft's constructions exclude all levels of security other than the extremely high "truly secure," not because the claims specify this high level of security (they are silent regarding the particular level of security required and do not mention "true" security), not because the specification requires such an interpretation (it describes varying degrees of security) and not because the ordinary meaning of the claim terms requires such an interpretation (Microsoft acknowledges its definition of "secure" is not standard).

Instead, Microsoft excludes all levels of security other than the highest possible level because, according to Microsoft, only the highest possible level is consistent with the "VDE invention." Microsoft contends that lower security embodiments should be ignored during claim construction, because in some places the specification uses the word "invention" in combination with VDE, thereby allegedly requiring that 115 pages, including "literally hundreds" of limitations, be read into every claim.

Microsoft's requirement that the "VDE invention" be imported into every claim leads Microsoft to claim constructions that directly contradict the definition given to the same terms in the specification. For example, the specification describes two embodiments of "tamper resistant barrier," a higher-security hardware embodiment and a lower-security software embodiment. Both of these embodiments are identified in the specification as a "tamper resistant barrier." Microsoft, however, demands that the claim term "tamper resistant barrier" be defined to exclude the software embodiment, since the software embodiment is inconsistent with Microsoft's requirement that VDE "true security" be read into every claim. Similarly, the specification describes two embodiments of "protected processing environment," a higher-security hardware embodiment and a lower-security software embodiment, both identified in the specification as a "protected processing environment." Microsoft's construction of "protected processing environment" excludes the software embodiment, again because this is inconsistent with Microsoft's requirement that VDE "true security" be read into every claim element.

The Federal Circuit has held that claim constructions that exclude disclosed embodiments are "rarely, if ever" correct. Microsoft's "VDE invention" construction of the claims ignores specification embodiments describing levels of security different than extremely secure "true" security, and contradicts the specification's use of the claim terms. Microsoft's construction must therefore be rejected as being inconsistent with the patent specifications.

II. ARGUMENT

A. Microsoft's Requirement of Absolute, "True" Security Contradicts the Specification.

1. Microsoft's VDE construction requires that the claims be interpreted to require an extremely high degree of security.

Microsoft's proposed constructions require that "each type of property identified in the patents is 'truly secure' against all types and levels of threats identified in the patents." MS Br., 28:1-2. According to Microsoft, this requires that "all users" are "guaranteed that all information, processes, and devices" will have five separate properties "maintained against all of the identified threats thereto." MS Br., 28:2-5. Microsoft justifies this extreme position by arguing that none of the patents excludes what Microsoft characterizes as "true security." MS Br., 28:7-17. Thus, Microsoft's brief includes statements such as the following:

> [T]he Big Book promises "**true" security**. It promises the ability to "prevent" unauthorized uses, etc., and "ensure" that rights will be enforced, and "guarantee" trustworthiness, even when faced with strong, sophisticated attacks against high-value content. Nothing in the claims indicates an inability to live up to these promises and protect such high-value content against such strong attacks.

MS Br., 32:16-20 (emphasis added). See also Id., 3:4-11, 17:4-6.

Microsoft asks that claims be interpreted narrowly so as to exclude all levels of security other than this "true" security, security so high as to amount to an absolute "guarantee" of protection against all threats, "no matter what effort may be made" to break the protection.

2. The specification discloses embodiments that do not require the highest degree of security.

As Microsoft acknowledges, the patents describe a variety of levels of security. Thus, Microsoft states that the patents use "secure" "to mean different things in different places," (MS Br., 25:18-19), and "the term 'secure' is used in the specification to refer to different things in different contexts." MS Br., 27:10-11.

The passage Microsoft relies upon for its requirement of "true" security makes exactly this point:

> The SPU 502 may be used to perform all **truly secure** processing, whereas one or more HPEs 655 may be used to provide **additional secure (albeit possibly less secure** than the SPE) processing . . . **Any service may be provided by such a secure HPE** . . . .

'193 patent, 80:30-36 (JCCS Ex. C, 22(B) (emphasis added).

Other passages similarly indicate that different degrees of protection may be desirable in different contexts:

> Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), **at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated** and/or the cost of an SPU 500 cannot be tolerated, **the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs** 655 executing on general-purpose CPUs 654.

'193 patent at 80:65-81:8 (JCCS Ex. C, 19(N)) (emphasis added). Additional examples of specification passages describing security levels below the highest level are found at JCCS Ex. C, 19(B), (C), (J), and (M).

Thus, the parties agree that the patent specification describes different degrees of security, including "truly" secure and "less" secure. The word "secure" is used to refer to both of these levels.

3. The patent claims do not specify a high degree of security.

The claims do not require "true" security. Both disclosed embodiments (truly secure and less secure) are within the scope of the word "secure" as used in the specification.

That "secure" is used to refer to different levels and degrees of security supports InterTrust's definition, since that definition allows such different degrees. Microsoft, however, argues that the breadth given to the term in the specification actually supports reading the most extreme disclosed embodiment into the claims, on the theory that the claims do not "exclude" this embodiment. MS Br., 28:12-13.[1] Microsoft further alleges that the context of the claims requires "true security" against "high-value, strong attack situations." MS Br., 28:9-17.

Microsoft fails, however, to adequately explain how the "context" of any particular claim requires the highest degree of security described in the patent specification. Claim 193.1, for example, involves downloading and playing music. This hardly seems the type of "high value, strong-attack" situation Microsoft describes. Microsoft gives no reason for assuming that the value and potential threats applicable to downloading songs is the same as the value and threats relevant, for example, to corporate trade secrets, nuclear weapons codes, money wire transfers, etc.

4. Microsoft's massive definition of "secure" invites the Court to usurp the jury's role in conducting the infringement analysis.

"Secure" is a general term, and the degree of protection necessary for a system to be "secure" depends on the context. The parties are in agreement on this, as is the specification.

When a claim term is drafted in general terms that may cover a range of circumstances, the Federal Circuit mandates that the Court construe the term generally and leave the question of determining whether an accused product meets that general construction to the finder of fact:

> Claims are often drafted using terminology that is not as precise or specific as it might be. . . . That does not mean, however, that a court, under the rubric of claim construction, may give a claim whatever additional precision or specificity is necessary to facilitate a comparison between the claim and the accused product. Rather, after the court has defined the claim with whatever specificity and precision is warranted by the language of the claim and the evidence bearing on the proper construction, the task of determining whether the construed claim reads

[1] InterTrust agrees that the claims do not exclude the "true security" embodiment. That claims do not exclude an embodiment obviously does not mean the claims require that embodiment.

> on the accused product is for the finder of fact.
>
> The proper allocation of the tasks of construing a claim and determining infringement in a case in which a claim contains an imprecise limitation is demonstrated by our decision in Modine Mfg. Co. v. United States Int'l Trade Comm., 75 F.3d 1545, 37 U.S.P.Q.2D (BNA) 1609 (Fed. Cir. 1996). In Modine, the patentee had claimed a condenser for an automotive air conditioning system with "relatively small" hydraulic diameters. Id. at 1549. From the specification and prosecution history of the patent, this court concluded that the term "relatively small" should be interpreted as referring to a range of diameters of "about 0.015-0.040" inches. Id. at 1554. Instead of attempting to define that range more precisely, we remanded the case for a factual determination of whether the claim limitation was literally infringed by accused products having diameters ranging from 0.0424 to 0.0682 inch. Id. at 1554-55.
>
> [T]he '886 patent contains some inherent imprecision resulting from the use of the term "consisting essentially of." As PPG points out, it is possible that under such circumstances different finders of fact could reach different conclusions regarding whether the effect of a particular unlisted ingredient in an accused product is material, and thus whether that product infringes. That possibility, however, is a necessary consequence of treating infringement as a question of fact subject to deferential review. It does not mean that the claim was improperly construed as an initial matter.

PPG Indus., Inc. v. Guardian Indus. Corp., 156 F.3d 1351, 1355 (Fed. Cir. 1998) (citation omitted).

PPG Industries is controlling here. "Secure" is a general term, the applicability of which depends on the context. The parties agree on this, and the patents describe different levels of security. The Court should, therefore, construe the term generally, and allow the jury to determine whether, under the particular circumstances, an accused product is or is not "secure."

B. Microsoft's VDE-Based Interpretation Requires Excluding Disclosed Embodiments.

The Federal Circuit is clear on constructions that exclude disclosed embodiments:

> A claim construction that does not encompass a disclosed embodiment is thus "rarely, if ever, correct and would require highly persuasive evidentiary support." Vitronics, 90 F.3d at 1583, 39 U.S.P.Q.2D (BNA) at 1578.

Johns Hopkins Univ. v. CellPro, Inc., 152 F.3d 1342, 1355 (Fed. Cir. 1998) (emphasis added).

Microsoft's VDE-based constructions lead to exactly this result.

1. Tamper-Resistant Barrier.

Microsoft argues that "tamper resistant barrier" must be interpreted as a hardware device. MS Br., 30:22-23. As Microsoft acknowledges, however, "the Big Book also refers to a 'tamper resistant barrier' which is not a physical hardware device." MS Br., 32:13-14.[2] In fact, the patent discusses this software embodiment at length, using the phrase "tamper resistant barrier" to refer to it. JCCS Ex. C, 22(B). Microsoft would thus have the Court construe "tamper resistant barrier" to exclude an embodiment identified in the specification as a "tamper resistant barrier." Why? Because defining "tamper resistant barrier" to include the software embodiment is inconsistent with VDE requirements Microsoft seeks to read into all of the claims (e.g., "true security," hardware Secure Processing Unit"). MS Br., 32:13-34:4.[3]

Microsoft's VDE construction is inconsistent with interpreting "tamper resistant barrier" to include the software "tamper resistant barrier." The Court therefore has a choice: accept Microsoft's VDE argument and construe this term in a manner contradicting the specification, or reject Microsoft's VDE construction and construe the term as it is used in the specification. As the Federal Circuit has held, the former of these approaches is "rarely, if ever" correct.

Moreover, InterTrust is aware of no Federal Circuit case that has ever held that a claim term can be interpreted to exclude, not merely a disclosed embodiment, but a disclosed embodiment that is identified in the specification using exactly the same words as the claim ("tamper resistant barrier"). Yet this is the result mandated by Microsoft's VDE construction.[4]

2. Protected processing environment.

Microsoft acknowledges that the specification discloses two embodiments of a protected processing environment, a hardware-based SPE and a software-based HPE, both of which are

[2] Microsoft also alleges that the "ordinary meaning" of tamper resistant barrier connotes a physical device (MS Br., 30:24-28), but neither of its experts testifies to this effect, and Microsoft's only support is a misleading citation to Dr. Reiter, testimony that Dr. Reiter explicitly characterized as "an example." Reiter I, 137:22. (Keefe Decl., Ex. E.)

[3] Microsoft also alleges in a conclusory manner that a software tamper resistant barrier would be too vague since "there would be no objective measure for distinguishing between a barrier which is tamper resistant and one which is not tamper resistant" (MS Br., 32:7-9), but fails to discuss the lengthy specification disclosure discussing the software tamper resistant barrier (JCCS Ex. C, 22(B)), nor does Microsoft address why a tamper resistant barrier provided by software requires an "objective measure" whereas no such objective measure is required for a hardware barrier.

[4] Moreover, the claim itself is inconsistent with Microsoft's interpretation. 721.1 recites not one but two tamper resistant barriers, and further recites that they have different security levels. The claim therefore clearly contemplates the possibility that one tamper resistant barrier will be more secure than another. For example, in one obvious embodiment, the first tamper resistant barrier would be hardware (higher security) and the second would be software (lower security).

explicitly identified as "protected processing environments." MS Br., 34:3-14. As Microsoft further acknowledges, Microsoft's definition of "protected processing environment" excludes the software-based HPE embodiment. MS Br., 35:3-14.

According to Microsoft, this is mandated for the same reason as exclusion of the software "tamper resistant barrier" from the construction of that term. MS Br., 35:12-14. Again, Microsoft's VDE-based construction requires excluding a disclosed embodiment from the definition of a claim term, even though that embodiment is <u>explicitly identified in the specification</u> using the exact same term, and even though the specification explicitly states that "any service" may be provided by a secure HPE. '193 Patent, 80:35-36 (JCCS Ex. C, 22(B)).

Interpretation of claim terms so as to exclude embodiments distinctly described in the specification is clear legal error, yet this is precisely the result of Microsoft's VDE-centric position.

C. Microsoft's Legal Arguments Are Misleading.

Microsoft's General Claim Construction Legal Analysis cites sources for the proposition that claims must recite the invention described in the specification. MS Br., 9:14-26. Microsoft emphasizes the word "invention" in these quotations, apparently hoping the Court will conclude that these cases and statutes stand for the proposition that, when the specification uses the word "invention," every element described thereafter must be read into every claim.

In fact, none of the cited authority supports this proposition. That claims must recite the invention described in the specification does not mean that when a patent specification uses the word "invention," the specification is automatically imported into the claims. InterTrust cited numerous Federal Circuit cases in its opening brief holding that elements described as the "invention" should not be read into the claims. InterTrust's Opening Br., 9:1-10:24. Microsoft does not even attempt to distinguish this authority.

D. Microsoft's Argument that the Claims Require VDE is Wrong.

1. '193 patent claims.

The '193 patent's claims do not refer to "VDE," nor to any other coined terms, such as "protected processing environment" or "host processing environment." In its attempt to shoehorn VDE into these claims, despite the absence of any VDE language, Microsoft relies on a variety of arguments that it repeats with respect to the other claims. First, Microsoft argues that the claims require elements that are not present in the claims themselves:

> All four '193 Patent mini-Markman claims concern the distribution and protection of digital content, and contemplate multiple nodes and participants. Information is received (**possibly** from multiple upstream content providers), then stored on a device having **unspecified** authorized and unauthorized users, and then conditionally transferred to another device having **unspecified** users.

MS Br., 16:22-26 (emphasis added).

Why are the multiple content providers and multiple users "possible" and "unspecified?" <u>Because the claims do not require them</u>. The claims do not refer to multiple upstream content providers. The claims do not refer to multiple users of the first device, much less authorized and unauthorized users. The claims do not refer to multiple users of the second device.

The InterTrust claims are silent on these questions. The claims are <u>consistent with</u> multiple upstream content providers, but do not <u>require</u> them. The claims are <u>consistent with</u> multiple users of the first device, but do not <u>require</u> them. The claims are <u>consistent with</u> multiple users of the second device, but do not <u>require</u> them.

That claims are consistent with a particular embodiment is hardly grounds for reading every limitation from that embodiment into the claims.

Prof. Maier's Declaration includes testimony that is apparently intended to buttress Microsoft's argument. That testimony is worth quoting in full:

> Additional **compelling evidence** of the presence of the Virtual Distribution Environment can be found in the process described in the claims themselves. For example, '193 Patent claim 1 purports to describes a distribution process involving at least three nodes. Thus, "receiving a digital file" implies, although does not explicitly state, that the digital file must come from some source device or system regardless of the transmission mechanism. Logically, this would be a system other than the "first device" and the "second device" which are described in other steps of the claim. Otherwise, the claim would have questionable utility.

Maier Decl., 23:17-25 (emphasis added).

This is typical of Microsoft's Markman positions in general. Prof. Maier establishes that a "received" digital file must come from somewhere (a point not disputed by InterTrust), but fails to explain why this is "compelling evidence" that the claims require VDE. Calling something "compelling evidence" does not make it so.

Microsoft's argument proceeds as follows:

> This claim language (e.g., "if . . . allows," "determining whether") is not qualified. It implies that if the copying and storing are not allowed, then they are prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made to take the unauthorized action. In other words, these claims imply that their "controls" are effective in the face of the attacks identified in the Big Book.
>
> These claimed protections against misuse cannot be achieved by encrypting the content. Encryption would not prevent the content from being accessed, copied, distributed, or stored. For these types of protection, "access control" is necessary. More particularly, the Big Book describes only the complete "invention" as providing such protection against the threats identified in the Big Book. In other words, by promising the type of effective access control protection said to be provided only by the complete VDE, these claims invoke that "invention."

MS Br., 17:4-14.

This passage is typical of Microsoft's reasoning. First, it is almost entirely devoid of evidentiary citations. The only citation that Microsoft makes is to four pages of Dr. Reiter's deposition testimony, testimony that Microsoft has not even put into evidence (it is excluded from the Keefe Decl.). Microsoft's failure to provide this testimony to the Court is understandable, since Microsoft has grossly mischaracterized the passage, in which Dr. Reiter explicitly disclaimed any requirement of absolute protection. Reiter II, 177:18-178:11. Declaration of Jeff McDow in Support of InterTrust's Claim Construction ("McDow Decl."), ¶ 2 and Ex. A.

Moreover, this passage is typical of Microsoft's arguments, since it piles inference on inference, none of them supported in any manner. Microsoft's chain of reasoning is as follows:

(1) The claims use the words "allows" and "determining," and do not qualify them.

(2) The absence of qualification means that the protections must be effective "no matter what effort may be made to take the unauthorized action." Microsoft makes this allegation, but does not even allege that one of ordinary skill in the art would have understood the apparently innocuous terms "allows" and "determining" to require absolute protection.

(3) The requirement of absolute protection means that the controls must be "effective in the face of the attacks identified in the Big Book." Microsoft makes no allegation that every

attack described in the patent specification is relevant to these particular claims (e.g., music downloading), nor does it explain why every possible attack must be protected against.

(4) The requirement of absolute protection against all types of attacks "cannot be achieved by encrypting the content. Encryption would not prevent the content from being accessed, copied, distributed or stored." Again, Microsoft presents no evidence for this proposition. Why, for example, would encryption not prevent content from being "accessed?" Microsoft doesn't say. Moreover, the claims themselves don't say anything about either the presence or the absence of encryption, and InterTrust has never alleged that the claims require encryption (nor that they exclude encryption for that matter).

(5) Since encryption is not sufficient, "[f]or these types of protection, 'access control' is necessary." The claims do not mention "access control." No Microsoft witness testifies that one of ordinary skill in the art would have understood these claims as requiring "access control." Instead, Microsoft imports "access control" into the claims because "access control" is allegedly better than encryption (also not mentioned in the claims) at ensuring the absolute degree of protection (also not mentioned in the claims) allegedly required by "allows" and "determining."

(6) Since access control is required, the claims invoke VDE:

Microsoft's argument reaches its conclusion in the following passage:

> More particularly, the Big Book describes only the complete "invention" as providing such protection against the threats identified in the Big Book. In other words, by promising the type of effective access control protection said to be provided only by the complete VDE, these claims invoke that "invention."

MS Br., 17:11-14.

This is a masterpiece of conclusory reasoning. "Such protection" is not mentioned in the claims, but is implied by Microsoft. The "threats identified in the Big Book" are not mentioned in the claims, but are implied by Microsoft. The claims do not make any type of "promise." This is implied by Microsoft. The claims do not mention "access control," either "effective" or non-effective. This is implied by Microsoft.

All of this, it should be recalled, rests on a rather thin reed: the presence of the words "allows" and "determining," in the claims, yet Microsoft provides no basis for concluding that one of ordinary skill would have interpreted these terms as implying hundreds of VDE limitations.

2. '683, claim 2.

Microsoft's justification for concluding that 683.2 should be interpreted as requiring the "hundreds" of VDE limitations is the following

> This claim [683.2] also concerns a multi-node distribution system. Here, "secure containers" and "secure container rules" are distributed amongst various nodes. The claim appears to promise the ability to prevent access to or use of protected information, using the secure containers, secure container rules, and a "protected processing environment." (See Second Mitchell Decl. at 6-7). These protections are not qualified as to the nature or severity of the threat being faced; they impliedly are effective against all threats identified in the patent or Big Book. The only system described in the Big Book or '683 Patent said to accomplish such protections, is the complete VDE. This claim further invokes VDE by using VDE and vague terminology, such as "secure container" and "protected processing environment."

MS Br. 17:27-18:1.

The only support cited by Microsoft for this characterization of 683.2 is the Second Mitchell Decl. at 6-7. Those Declaration pages do not discuss this claim.

Microsoft's key argument is the following: "These protections are not qualified as to the nature or severity of the threat being faced; they impliedly are effective against all threats identified in the patent . . . ." Microsoft does not explain why an absence of qualification means the claims require the highest degree of security (as opposed to the lowest, or to the security relevant under the circumstances). Nor does Microsoft explain how this implication can be squared with specification statements that security may be limited, may be broken, or may consist of fewer than all protection mechanisms. JCCS Ex. C, 19(A)-(N), 19(Q)-(T).

3. '721, Claims 1 and 34.

Again, Microsoft's argument consists entirely of conclusory allegations. Microsoft argues that "The '721 Patent purports to improve the Big Book VDE by preventing the use of executable code (specifically "load modules" in Claim 1) except as authorized." MS Br., 18:8-9. No citation is given for this assertion, and Microsoft makes no attempt to tie it to the claims, other than noting that 721.1 recites load modules.

Microsoft continues by alleging that "Such prevention requires an access control capability." MS Br., 18:9-10. Again, no citation is provided, and neither claim mentions any such capability.

Microsoft then argues that the claims "promise such protections without any qualification." MS Br., 18:10-11. The claims contain no such promises, and Microsoft fails to explain why an absence of qualification requires the highest possible degree of protection.

Microsoft ends by arguing that the claims "invoke the 'invention'" by including the terms "protected processing environment," "tamper resistant barrier" and "security." As is discussed above, the first two of these are described using higher-security and lower-security embodiments, so these terms hardly support a requirement that the claims be interpreted using the highest possible security level. As to the word "security," this is a common word, and Microsoft provides no basis for reading a requirement of "VDE" into this term, other than the implication that VDE is the "context," an argument that is inconsistent with the multiple embodiments disclosed in the patents.

4. Other claims.

Microsoft's arguments regarding the other claims suffer from the same infirmities and should be rejected for the same reasons as discussed above.

E. Microsoft's Bases for Reading the Specification Into the Claims Are Either Mischaracterized or Do Not Apply.

Microsoft identifies various situations in which Microsoft believes that limitations can be read from the specification into the claims. MS Br. at 11:27-14:15. These situations are either mischaracterized by Microsoft or have no relevance to this case.

(1) To provide clarity. Microsoft cites cases for the proposition that, if a particular claim term deprives the claim of clarity, the court may look to the specification for guidance in interpreting the claim. MS Br., 11:27-12:13. Each of the cases cited by Microsoft concerned a particular interpretation issue raised by a particular claim element (e.g., does "automation code" mean particular code in an operating system? (Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1374-75 (Fed. Cir. 2003)); does "coupling" require different voltages? (NeoMagic Corp. v.

Trident Microsystems, Inc., 287 F.3d 1062, 1071-72 (Fed. Cir. 2002)); does "sealingly connected" require misaligned taper angles? (Watts v. XL Sys., Inc., 232 F.3d 877, 882-83 (Fed. Cir. 2000)); does "without significant cross-linking" include a particular type of cross-linking? (North Am. Vaccine v. American Cyanamid Co., 7 F.3d 1571, 1575-76 (Fed. Cir. 1993)).[5]

None of these cases involved an attempt by a patent defendant to read hundreds of limitations into every claim, nor to interpret numbers of claim terms using significant limitations that are not tied to any use of the terms themselves in the specification.

(2) Express or implied definition in the patent. Most of the cases cited by Microsoft involve an explicit definition in the patent or file history. Notably, where such definitions have been provided in the present case, Microsoft has chosen to ignore them (e.g., Device Class, Contained).

As Microsoft points out, the cases involving an "implied" definition concerned use of a claim term "throughout the entire patent specification in a manner consistent with only a single meaning." MS Br., 12:19-20. In this case, however, Microsoft makes no attempt to establish that any particular claim terms are used consistently with only one meaning. Indeed, Microsoft regularly notes that the specification uses claim terms in multiple manners, or in a manner inconsistent with Microsoft's proposed interpretation (e.g., "tamper resistant barrier," "protected processing environment").

(3) Important to the Invention. This issue is addressed in InterTrust's opening brief. That specification characterizations of "the invention" do not constitute a magic formula automatically pulling the specification into the claims, however, is made clear by the cases cited in InterTrust's opening brief, each involving specification statements about "the invention," each holding that those statements did not limit the claims. Microsoft does not even attempt to distinguish these cases.

Microsoft's characterization of SciMed Life Sys. v. Advanced Cardiovascular Sys., 242 F.3d 1337 (Fed. Cir. 2001) is at best disingenuous: "limiting claim term 'lumen' to 'coaxial

[5] One of the cases cited by Microsoft (Ethicon Endo-Surgery v. United States Surgical Corp., 93 F.3d 1572 (Fed. Cir. 1996)) is miscited, since the Federal Circuit used the prosecution history,

lumen' in part because the specification characterized the coaxial configuration as part of the 'present invention.'" MS Br., 13:7-9. In fact, as InterTrust pointed out in its opening brief, the Scimed patent went well beyond characterizing this element as "part of" the invention: the specification stated that the element was present in **"all embodiments"** of the invention, a statement the Federal Circuit characterized as "the most compelling portion of the specification," a statement that significantly exceeds anything present in the current case. 242 F.3d at 1343.

In addition, the cases cited by Microsoft involved specific issues relating to specific terms (Scimed: does "lumen" mean "coaxial lumen?"; Toro Co. v. White Consol. Indus., 199 F.3d 1295, 1300-01 (Fed. Cir. 1999): does "including" mean "attached?"). Neither case held that statements about the "invention" required that an entire embodiment with hundreds of limitations be incorporated wholesale into every claim.

(4) Distinguishing prior art. Microsoft argues that statements distinguishing prior art may support reading embodiments into the claims. MS Br., 13:10-20. Cases cited by Microsoft generally concern file wrapper estoppel, Spectrum Int'l v. Sterilite Corp., 164 F.3d 1372, 1378 (Fed. Cir. 1998); Rheox, Inc. v. Entact, Inc., 276 F.3d 1319, 1325-26 (Fed. Cir. 2002).[6]

The one case cited by Microsoft that does relate to a specification statement illustrates why this doctrine does not apply in the present case. In Innovad, Inc. v. Microsoft, 260 F.3d 1326 (Fed. Cir. 2001), the court construed the claim term "dialer" in light of a specification statement that prior art dialers of a particular type were "useless" for a particular purpose. On that basis, the court concluded that the claim term "dialer" should exclude that particular type.

Here, in contrast, Microsoft points to no specification statement discussing a specific claim term in light of the prior art. For example, there are no specification statements to the effect that prior art software tamper resistant barriers were inadequate for some particular purpose. Nor does Microsoft cite any case standing for the proposition that a general statement about the inadequacies of the prior art and the advantages of an overall embodiment described in

rather than the specification, to interpret the claim element. 93 F.3d at 1579-80.

[6] CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366-67 (Fed. Cir. 2002) includes this factor in a list of possible factors but does not apply it, though it does cite the Spectrum file wrapper language.

the patent requires that every detail of that embodiment be read into every claim. Nor does Prof. Mitchell's testimony about various references fill this gap, since he does not tie his discussion of these references to any particular specification statement that distinguishes them. Mitchell 2nd Decl., 10:17-18:4.

(5) Express disclaimer. Microsoft does not argue that any express disclaimer exists.

F. Microsoft's Argument about the InterTrust Divisionals Misses the Point.

In its opening brief, InterTrust pointed out that the Patent Office's restriction requirement demonstrated that the foundational InterTrust application involved multiple inventions, inventions that the Patent Office expressly held related to separate classes, each shown to be "separately usable." InterTrust Opening Br., 11:5-12:20. This determination rebuts any argument that the original InterTrust specification disclosed only a single VDE "invention."

Microsoft makes arguments in response, but none to the point. Microsoft argues that the Patent Office's restriction requirement is irrelevant because "InterTrust's patent claims are free to recite additional features, which additional limitations may (or may not) make them separate 'inventions' under Patent Office restriction practice. But, that is not the issue here." MS Br., 15:3-7.

Microsoft does not explain why "that is not the issue here," and it certainly seems to be the issue: Microsoft argues that the patents disclose a single, unitary VDE invention, and hundreds of limitations must be read into every claim. Microsoft relies heavily on statements referring to "the invention," and argues that "the invention" must be incorporated into every claim. The restriction requirement, however, makes it clear that references in the application to "the invention" cannot be read as meaning that the application recited a single invention.

Microsoft also points out that divisional patents may end up with claims directed to the same invention, and that in such a case the resulting patents are invalid. Microsoft further argues that, because the claims of the divisional applications were changed, the presumption they were directed to different inventions should not apply, citing Gerber Garment Tech., Inc. v. Lectra Sys. Inc., 916 F.2d 683 (Fed. Cir. 1990).

Gerber includes no such holding, nor could it, since the presumption of patent validity is statutory, and cannot disappear merely because a divisional application's claims have been changed. The Court must presume that the Patent Office acted properly in the original restriction requirement, and in issuing the subsequent patents, including the amended claims. Thus, the Court must presume that the divisional applications were originally drawn to different inventions, and that the subsequent patents issuing from those applications were also drawn to different inventions, since otherwise the divisional patents would be invalid, and those patents carry a statutory presumption of validity.

Microsoft characterizes Ballard Med. Prod. v. Allegiance Healthcare Corp., 268 F.3d 1352 (Fed. Cir. 2001), as follows: "limiting claims of both a patent issued from the parent application and a patent issued from a divisional of such parent to exclude a particular type of valve based on statements made in common specification text and prosecution history of the parent application." MS Br., 15:26-16:2. This is wrong. In Ballard, the Federal Circuit held that statements in a parent prosecution history can serve to limit later patents. 268 F.3d at 1361-62. No issue of statements made in the specification was raised in the case. In particular, the Federal Circuit did not address specification statements about "the invention."[7]

G. Individual Claim Elements.

1. Microsoft ignores ten claim elements.

Microsoft filed a forty page brief, plus two expert Declarations, but neither Microsoft nor its experts have anything to say about ten of the thirty terms at issue in this hearing: (1) Aspect, (2) Authentication, (3) Compares, (4) Derive, (5) Designating, (6) Device Class, (7) Digital Signature/Digitally Signing, (8) Executable Programming/Executable, (9) 721.1: "digitally signing a second load module...." (10) 912.8: "identifying at least one aspect of an execution space required for use and/or execution of the load module."

[7] Moreover, Ballard involved claims interpreted under 35 U.S.C. § 112(6), which are supposed to be limited to the embodiments disclosed in the specification, so this case would be distinguishable even if Microsoft had correctly characterized it. 283 F.3d at 1359-60.

2. Use.

InterTrust's definition is taken from a standard dictionary (JCCS, Ex. C, 23(A)). The Federal Circuit approves using dictionary definitions. Inverness Med. Switz. GmbH v. Princeton Biomeditech Corp., 309 F.3d 1365, 1369-70 (Fed. Cir. 2002).

Microsoft's argument on "use" is mysterious, as Microsoft concentrates on "encryption," and on a series of alleged InterTrust contentions. MS Br., 20:6, 21:20-25. Encryption appears irrelevant to the proposed definitions, and InterTrust never made the contentions.

3. **Copy.**

Microsoft responds at length to arguments never made by InterTrust, and ignores InterTrust's central point: Microsoft's definition would result in a nonsensical interpretation of 193.1, in which a budget for making copies would be used up by "phantom," internal reproductions that the user would never know existed, much less be able to use. Microsoft does not attempt to explain how its interpretation would make sense in the context of the claim.[8]

4. **Secure/Securely.**

Microsoft acknowledges that its proposed definition is neither "standard" nor an express definition from the patent. MS Br. at 28:6-7. What Microsoft fails to acknowledge is that its definition actually contradicts the specification. According to Microsoft, a system is secure only if it protects five separate properties against attack, and only if this protection is 100% effective. As described above (§ II A 2), however, the specification explicitly describes various levels of security, and characterizes them all as "secure."

Microsoft attacks InterTrust's definition, arguing that InterTrust ignores the effectiveness of the efforts taken. MS Br., 26:10-11. In fact, InterTrust's proposed definition requires that the mechanisms employed "prevent," "detect" or "discourage" misuse or interference. A mechanism that fails to perform these functions (e.g., a completely ineffective mechanism) would not be "secure" under InterTrust's definition.

[8] Prof. Mitchell's commentary on "copy" is similar: a great deal of discussion of this phrase in the abstract, but no attempt to explain how Microsoft's proposed definition would make sense in the context of the claim, nor any attempt to respond to InterTrust's discussion of this in its opening Brief. Mitchell 2nd Decl., 6:23-8:2.

Microsoft also argues that VDE "promises the ability to prevent" various types of misuse, and that detecting or discouraging misuse is not security. MS Br. at 26:14-20. Microsoft cites no support for this proposition, and it is clearly incorrect. In some circumstances, mechanisms that allow the detection of misuse are fully sufficient for security. For example, technology that made it possible to detect an alteration of a driver's license would render the driver's license "secure," since, although the driver's license could be altered (e.g., to change the birthdate of an underage would-be drinker), the fact that the change could be detected would make it impossible for an attacker to gain any benefit from the misuse.

Thus, one disclosed embodiment of the tamper-resistant barrier "detects tampering and/or destroys sensitive information." JCCS Ex. C, 22(A). It is impossible to read this passage of the specification as requiring any protection mechanism other than "detection."

Microsoft also mischaracterizes Dr. Reiter's testimony, alleging he testified that none of the five listed forms of protection is required. MS Br., 27:1-3. As with so many of Microsoft's citations, however, this one is false. In the cited passage from Dr. Reiter's deposition, a Microsoft attorney asked a series of questions, each question relating to a single mechanism. Since security requires one or more of these mechanisms, but does not require all of them, Dr. Reiter correctly answered "no" when asked whether the claims required each mechanism in isolation. Dr. Reiter was never asked whether at least one mechanism from the entire group was required, and he never testified that security could exist without any mechanism at all. Reiter 202:5-204:14 (McDow Decl., Ex. A.)[9]

5. Secure Container.

Microsoft alleges that only a single embodiment is disclosed, and that it requires the ACCESS method. MS Br., 29:10-13. This is false. The ACCESS method excerpts quoted by Microsoft are part of a longer passage that is expressly described as being an "an example" ('193 patent, 192:2), and the same passage describes the ACCESS method Microsoft cites as a

[9] Similarly, suppose a movie theater offered half-price tickets to customers ages ten to twelve, and a particularly obtuse customer posed the following series of questions: "Do I have to be 10 to receive the discount?" "Do I have to be 11 to receive the discount?" "Do I have to be 12 to receive the discount?" The answer to all three questions would be "no," but this obviously

"complicated procedure" and notes that "in many cases" a "relatively trivial" procedure may be used instead. Id. at 192:6-11.

In addition, Microsoft argues that the "access control ability of VDE secure containers" is "critical to VDE's promise to content owners." MS Br., 28:3-7. The phrase "VDE secure container" does not appear in the '193 patent. McDow Decl., ¶ 3. When the inventors wanted to refer to a container in terms of VDE capabilities, they explicitly identified it as a "VDE container" (e.g., JCCS Ex. C, 20(E)). The patent claims do not refer to "VDE containers," but instead refer to "secure containers."[10] Microsoft seeks to confuse this issue by using the phrase "VDE secure containers;" in an apparent attempt to mislead the Court into believing that "secure containers" and "VDE containers" are identical.[11]

6. Tamper Resistant Barrier.

As discussed above, Microsoft's construction of "tamper resistant barrier" admittedly excludes an embodiment that is referred to in the specification as a "tamper resistant barrier." Microsoft's argument also suffers from other defects. Microsoft alleges that the specification requires a hardware barrier wherever content is "assigned usage control information, or used." MS Br. at 33:10-14. Microsoft quotes several excerpts at length, none of which even mentions tamper resistant barriers, much less excludes software tamper resistant barriers.

Moreover, the term "tamper resistant barrier" is recited only in 721.34. Microsoft rather casually alleges that "all of the mini-Markman claims contemplate one or both of these two conditions" (i.e., assigning usage control information to content or using content). MS Br., 33:10-12. Claim 721.34 has no reference to assigning usage control information or any use of content, nor does it have any language from which such elements can be inferred.

wouldn't establish that the discount is an illusion.

[10] InterTrust agrees that "VDE containers" are one embodiment of "secure container," but this obviously does not mean that all "secure containers" are "VDE containers."

[11] Prof. Maier states that "I believe it is apparent that [secure container] is intended to refer to the VDE container." Maier Decl., 22:17-18. He gives no basis for this belief, nor does he explain how "secure container" is used in the specification, other than noting it only occurs twice in the '193 patent. This statement is itself misleading, since it ignores the extensive use of the term in the '683 and '861 patents, both of which include mini-Markman claims using "secure container." McDow Decl., ¶ 5.

In addition, Microsoft's argument that a hardware barrier is required ignores alternative embodiments described in the specification. For example, Microsoft ignores the excerpt cited by InterTrust at JCCS Ex. C, 22(B), which describes a "secure HPE" with a software tamper resistant barrier, and states that "Any service may be provided by such a secure HPE . . . ."

Prof. Maier alleges that the "tamper resistant barrier" recited in the claims is referred to as a "tamper resistant security barrier," or a "tamper-resistant hardware security barrier." Maier Decl. 34:21-23. The claim uses the term "tamper resistant barrier," rather than these other phrases. That the specification uses these other phrases to refer to hardware barriers is evidence that the unqualified phrase "tamper resistant barrier" should apply to both embodiments.

Prof. Maier acknowledges that the patent "alludes to" a software tamper resistant barrier, but he states that "the specification gives no indication how to determine what the boundaries of such a 'barrier' might be or how to implement such techniques successfully." Maier Decl., 35:7-10. The quotation (JCCS Ex. C, 22(B)) contains more than an "allusion" to a software tamper resistant barrier, it explicitly describes numerous techniques that may be used to provide one.

7. Protected Processing Environment.

Microsoft's main argument regarding this term is discussed above in § II B 2, and its other arguments amount to quibbles that InterTrust's definition is not specific enough. No claim construction can address every possible infringement issue. As the Federal Circuit has held, if a claim term is reasonably defined in general terms, it is the Court's obligation to adopt that construction, leaving the question of application of the general definition to the jury. PPG Industries, 156 F.3d at 1354-55.

8. Component Assembly.

Microsoft asserts that "In the Big Book the term 'component assembly' (also called 'component') uniformly is used to refer to executable components, which are an assembly of independent, executable load modules and data." MS Br. at 35:12-14. Microsoft provides no support for the assertion that a "component assembly" is also called a "component," an assertion that seems odd, since a "component assembly" is self-evidently an assembly of components.

Microsoft's main argument is that InterTrust's definition would allow the possibility of a component assembly that does not include any executable code. InterTrust did not intend to leave open the possibility that a component assembly might include no programming. InterTrust is willing to amend the third sentence of its proposed construction to read as follows: "Component Assemblies must include code, and are utilized to perform operating system and/or applications tasks."

Microsoft makes no attempt to otherwise defend its complicated definition.

Prof. Maier's discussion of "component assembly" notes that the specification describes multiple embodiments (Maier Decl., 17:1-3), but appears to consider this to be an improper practice. At a later point in his Declaration, Prof. Maier states that InterTrust's citations relating to "component assembly" all relate to VDE, though he only quotes language from two of these citations. Maier Decl., 27:2-10. Prof. Maier appears not to have appreciated the point of a number of these quotations: that the VDE-related description of "component assembly" is expressly and repeatedly referred to as a "preferred embodiment."

9. Control (noun).

Microsoft's argument includes an analogy relating to librarians, but without any support from the experts or the patents that this analogy is reasonable or correct. Thus, Microsoft argues that "rules" and "controls" should not be equated, on the basis that "rules" are non-executable, whereas controls are "executable." Microsoft presents no evidence for its assertion that "rules" are non-executable, other than the argument that "rules" constitute the "guard" in Microsoft's analogy.

Moreover, the quotations cited by Microsoft in its brief and in JCCS Ex. D do not state that a "control" must be executable, but instead are merely consistent with "controls" being executable programming, as is InterTrust's proposed definition.

Prof. Maier argues that "control" should be interpreted in light of VDE because 75% of the passages cited by InterTrust allegedly relate to VDE. Maier Decl., 28:2-3. Prof. Maier does not explain the significance of this statistic, and it does not seem to have occurred to Prof. Maier that the non-VDE uses constitute evidence that the term should not be limited to VDE.

10. A budget specifying the number of copies which can be made of said digital file (193.1).

Microsoft argues that InterTrust's construction does not specify "since when," "by whom" or "by what." The claim does not require this information, and Microsoft does not explain why a budget must include it.

11. Container.

Although Microsoft discusses this word separately (MS Br., 39:3-7), "container" is not a disputed term, but instead occurs as part of "secure container." InterTrust's definition of "secure container" rests on a definition of "container" from the Microsoft Computer Dictionary and is consistent with use of the term in the mini-Markman patents, and a contemporaneous Microsoft patent. JCCS Ex. C, 20(I), (J).

Microsoft argues that, in the patents, "container" is not used in the manner asserted by InterTrust, citing Alexander Decl. 20(A)-(D). Microsoft provides no explanation for why these passages are inconsistent with InterTrust's construction.

12. Containing.

The patent explicitly defines "containing" as including referencing. JCCS Ex. C, 7(B). Microsoft's argument about the "ordinary meaning" of the term is both unsupported and irrelevant in light of this explicit definition, and in light of the Microsoft Computer Dictionary definition for "container" ("a file containing linked or embedded objects"). JCCS Ex. C, 20(I).

13. Control (verb) / Controlling.

InterTrust's definition comes directly from a standard dictionary. Microsoft's only response is that this is inconsistent with VDE. Microsoft fails, however, to cite any text from the patents defining "controlling" in any particular manner, and the only quotation it includes does not even use "control" as a verb. As InterTrust pointed out in its opening brief, the patents use "control" as a verb in many non-VDE contexts. InterTrust Opening Br., 21:23-28.

14. "Controlling the copies made of said digital file" (193.1).

Microsoft does not attempt to support its proposed definition, which is long and complex. Instead, Microsoft quibbles about implications arising from InterTrust's construction.

The InterTrust construction is based on the manner in which this phrase is used in the claim, in which it explains the "copy control." See JCCS Ex. A, Row 7. The nature of the copy control is further described later in the claim. JCCS Ex. A, Rows 8 and 9. InterTrust's definition is based on the phrase itself and on its context in the claim, a context Microsoft entirely ignores.

15. "Derives information from one or more aspects of said host processing environment" (900.155).

Microsoft's argument consists of unsupported allegations, including the assertion that a "unique" signature is required, that "the derived information may serve no security purpose at all," and that this "is contrary to the patent." Microsoft's Ex. D evidence for this term consists of 122 separate citations amounting to twenty pages. Since Microsoft's allegations are not tied to any particular text, InterTrust cannot respond, other than stating that any text Microsoft may subsequently identify will simply be an embodiment, since this term occurs frequently in the passages quoted in Microsoft's JCCS Ex. D.[12]

16. Host Processing Environment.

In its opening brief, InterTrust acknowledged that its definition of Host Processing Environment does not include the "insecure" variant, and proposed an alternate definition. InterTrust Br., 36:13-19. Microsoft ignores this, criticizing InterTrust for failing to cover insecure host processing environments. MS Br., 40:10-13. Microsoft otherwise fails to respond to any of InterTrust's points on Host Processing Environment. InterTrust Br., 36:20-37:10.

17. Identifier.[13]

Microsoft claims that InterTrust's definition of "identify" is "contrary to the ordinary meaning." InterTrust's definition is from the American Heritage Dictionary. JCCS Ex. C, 17(F).

[12] If Microsoft subsequently identifies particular relevant passages, InterTrust will move to strike those identifications as being inconsistent with this Court's Patent Local Rules. It is one thing to make assertions that are supported by one or two pages of quoted text. It's quite another to make general arguments that are not supported by any individual citations but are instead allegedly supported by twenty pages of block quotes. The Patent Local Rules require the parties to identify relevant evidence. Twenty pages of unexplained quotes do not comply with this requirement.

[13] Microsoft's brief discusses "identifying (identify)," neither of which are terms to be construed in this proceeding. MS Br., 40:14. Since Microsoft also cites the JCCS Ex. A reference covering "identifier," InterTrust will assume that Microsoft is intending to discuss this term, and will respond accordingly.

18. Tamper Resistance.

Microsoft's argument consists of an unsupported assertion ("plainly is not what VDE means by 'tamper resistance'") and a quibble ("more than difficult [sic] than what?"). MS Br., 40:21-25. As to the former, assertions do not constitute evidence supporting Microsoft's construction. As to the latter, more difficult than if the tamper resistance were not present.

Prof. Maier, on the other hand, spends considerable time discussing this concept, including two pages of symbolic logic, apparently intended to prove that tamper resistance cannot include detection of tampering. Maier Decl., 32-34. However, whatever the details of Prof. Maier's analysis, he simply fails to address JCCS Ex. C 21(B), a quotation that explicitly states that a tamper resistant barrier "detects tampering and/or destroys sensitive information." This quotation clearly equates tamper resistance with detecting tampering, and does not require that tampering actually be blocked.

19. Budget.

Although Microsoft's brief does not refer to "budget," Prof. Maier's Declaration discusses this term, though without any citation to the claims or specification. Maier Decl., 17:6-13. Prof. Maier acknowledges that the specification sometimes uses "budget" to refer to data and in other places uses "budget" to refer to executables, but treats this as an "inconsistency" that leads to "confusion" (Maier Decl., 17:11) rather than as multiple embodiments that establish the term can refer to either data or an executable.

20. Clearinghouse.

Prof. Maier alleges that "clearinghouse" has "a specific meaning in the banking and commerce fields." Maier Decl., 24:1-2. Unfortunately, he fails to explain what this alleged meaning might be, or how it would support reading VDE features into the claims. Instead, he cites some quotations from InterTrust, but does not respond to a primary point made in InterTrust's opening brief: Visa and AT&T are identified in the specification as "clearinghouses," yet no one could believe that either Visa or AT&T have the various VDE features required by Microsoft's proposed definition.

H. Testimony Cited by Microsoft.

Exhibit A to the Keefe Declaration contains numerous quotations that Microsoft does not refer to in its brief. Most of these quotations are from inventors or third party deponents. The inventor testimony is not tied to the patents, and "The subjective intent of the inventor when he used a particular term is of little or no probative weight in determining the scope of a claim (except as documented in the prosecution history)." Markman v. Westview Instruments, Inc., 52 F.3d 967, 985-86, aff'd, 517 U.S. 370 (1996). The third party testimony suffers from the same defects as the testimony InterTrust moved to strike in connection with Microsoft's summary judgment motion, and is incompetent for those same reasons.

III. CONCLUSION.

Microsoft's VDE-centric claim interpretation would require the Court to ignore embodiments disclosed in the specification, and to interpret particular claim terms in a manner that excludes disclosed embodiments, a practice the Federal Circuit has held is "rarely, if ever," correct. Microsoft supports this extreme position with conclusory reasoning and egregious miscitations of the record.

Microsoft's claim constructions are longer and more complicated than any constructions ever adopted by any court. Those constructions would read literally hundreds of limitations into every single claim. InterTrust respectfully requests that the Court reject Microsoft's VDE-centric interpretation position and adopt the claim constructions proposed by InterTrust.

Dated: April 21, 2003

Respectfully submitted,

DERWIN & SIEGEL, LLP

By: ____________________
DOUGLAS K. DERWIN
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
KENNETH J. HALPERN (State Bar No. 187663)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA (MEJ) **REPLY TO INTERTRUST'S OPPOSITION TO MICROSOFT'S BRIEF IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT THAT CERTAIN "MINI-*MARKMAN*" CLAIMS ARE INVALID FOR INDEFINITENESS**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Page

Advanced Display System, Inc. v. Kent State University,
212 F.3d 1272 (Fed. Cir. 2000) 15

Amgen, Inc. v. Chugai Pharmaceutical Co., Ltd.,
927 F.2d 1200 (Fed. Cir. 1991) 14

Amgen v. Hoechst Marion Roussel, Inc.,
314 F.3d 1313, 1341-42 (Fed. Cir. 2003) 11

Ex parte Brummer,
12 U.S.P.Q.2d 1653 (B.P.A.I. 1989) 12

J.T. Eaton & Co. v. Atlantic Paste & Glue Co.,
106 F.3d 1563 (Fed. Cir. 1997) 10

Orthokinetics v. Safety Travel Chairs, Inc.,
806 F.2d 1565 (Fed. Cir. 1986) 12

STX, Inc. v. Brine, Inc.,
37 F.Supp.2d 740 (M. Md. 1999) 12

Ex parte Schwarze,
151 U.S.P.Q. 426 (B.P.A.I. 1966) 14

Union Pacific Resources Co. v. Chesapeake Energy Co.,
236 F.3d 684 (Fed. Cir. 2001) 1

United Carbon Co. v. Binney & Smith Co.,
317 U.S. 228 (1942) 15

FEDERAL STATUTES

35 U.S.C. § 112 .... 1, 11, 14

I. INTRODUCTION AND SUMMARY OF ARGUMENT

InterTrust's opposition brief throws up a storm of noise, diversion and straw arguments that should not distract this Court's attention from the very simple question on which the defense of indefiniteness will be determined: Whether the claim has sufficiently definite scope that a person of ordinary skill in the art can understand what it means in light of the specification and thereby determine what is outside its scope. *Union Pac. Resources Co. v. Chesapeake Energy Co.*, 236 F. 3d 684, 692 (Fed. Cir. 2001). For each of the eleven claims challenged on this motion, the answer must be, "No."

What emerges from InterTrust's opposition brief are two important points upon which the parties agree: First, "secure" is a relative term that has only a vague, general meaning in the art, which can mean different things in different contexts. Second, to determine what is "secure" in any particular context one of skill in the art needs specific criteria. The essential problem with InterTrust's patents is that they fail to provide the needed context and they fail to adopt any particular criteria, leaving both critical steps for others to guess at. They further fail to define "secure" expressly, and they fail to define it implicitly by identifying any particular technology used to achieve security. When one turns to the Big Book for resolution of the resulting ambiguity, it is like coming to a trailhead with 50 signs labeled "secure," but each pointing in a different, inconsistent, and often times contradictory direction.

The term "secure" is unusual in that it is a label characterizing a multidimensional condition of something – a result achieved amid constantly changing circumstances. It is an inherently subjective concept that can be evaluated in many different ways (with correspondingly different outcomes). Labels set forth in patent claims, however, must be subject to an objective evaluation. Otherwise, it is impossible for the public to evaluate the scope of the claim.

The ***claims*** fail to recite either context or criteria. The traditional places to which one turns to correct this shortcoming are equally unavailing. The evidence from the parties' experts, corroborated by third party accounts, confirms that definite context and criteria is critical information for anyone having skill in this art, and it is information that merely having skill in the art does ***not provide***. To the contrary, persons of skill in the art are aware of a multitude of possible ways of distinguishing between something that is "secure" and something that is "not secure." Finally, ***the specification*** is equivocal on everything except what "VDE" can do, and the file history offers no resolution. Indeed, the specification compounds the problem because it mentions but fails to adopt any of the many possible security contexts and criteria. After reading the nearly one thousand pages of Big Book text, the person of ordinary skill in the art would have no idea what, for example, a claim's "secure container," "secure memory," or "secure process" must protect, or against what threats, or to what degree, or by what criteria such evaluations should be conducted. The evidence from the parties' experts, corroborated by third party accounts, confirms that specific context and criteria are critical information for anyone having skill in this art, and it is information that merely having skill in the art does ***not provide***. It is for these reasons that the mini-*Markman* claims are indefinite and should be declared invalid.

II. "SECURE" AS USED IN THESE MINI-MARKMAN CLAIMS RENDERS THEM INDEFINITE

A. A Person of Skill Reading the Claims Cannot Tell What "Secure" Means in Light of the Relevant Art

One of skill in the art reading the claims finds references to "secure memory," "secure database," "secure container," "securely assembling," and "level of security," but no explanation of what is meant by "secure" other than the promises made for the "present invention," "VDE." Looking to the art as a whole for guidance offers no comfort. The term, *as InterTrust admits*, has only a very general meaning – that some designs, techniques or mechanisms are used to protect certain properties against some kind of attack or adversarial conditions. InterTrust Opp., at 4 (quoting Prof. Mitchell's definition as the one on which both parties' experts "agree"). This definition manifestly lacks a clear boundary. Which designs, techniques, mechanisms, properties, attacks, and or conditions are intended? The claims point to no criteria in the art that would answer that question.

Both parties' experts agree that criteria are needed to reach a precise understanding of "secure." The testimony of InterTrust's own expert, cited in Microsoft's opening brief, fully supports the proposition that the term needs further specification of parameters and criteria in order to be sufficiently definite.[1] Microsoft Brief, at 4. InterTrust's expert now adds that to apply the general meaning of "secure" "to a particular product or system, it is necessary to understand the context of that product or system." Reiter Decl., at ¶ 3. Dr. Reiter also admits that there are "several recognized methodologies for determining if computer products are 'secure'" and that "[c]omputer security professionals routinely use such methods to determine if products or methods are 'secure.'" Opp., at 3; Reiter Decl., at ¶ 3. InterTrust even approvingly characterizes Dr. Mitchell's testimony as meaning that one must know the protected properties and potential attacks to determine if a particular system is "secure," and that recognized methodologies are used to perform this investigation. *Id.* at 5. The Mitchell declaration, scholarly articles, and third-party witnesses have provided evidence to the same effect. *Id.*; Mitchell Decl., at 4-11.[2]

It should be noted here that InterTrust's allegation that Prof. Mitchell did not try to understand the terms in the context of the claims is based on a misrepresentation of his testimony. As Prof. Mitchell clearly explained, for each term and phrase in question, he "tired to look at its meaning in three different ways" – whether the term by itself has a commonly understood specific meaning, whether the term is clear "in the context of the claim," and whether the patent specification provides "any further information." (Mitchell Depo. at 294). In its brief, however, InterTrust cut off the quotation of Prof. Mitchell's testimony right before he gave an answer that contradicted the proposition for which InterTrust quoted him:

> A. I -- I tried to explain a little bit earlier that my task to this point in this case has been to, first of all, understand the patent's specs and so on, and, second, in particular to this declaration, think about these particular phrases, what they mean in general, what they appear to mean in the claims, and ponder the question of whether the specification gives us additional useful information so that I could pin down the meaning of these terms in a useful and meaningful way.

[1] InterTrust erects Prof. Mitchell's effort to summarize the different axes of security into a classic straw man. Calling it a "test" – a term nowhere used by Microsoft – InterTrust reasons that, because this "test" is not recognized as such in the art, it sheds no light on the definiteness of InterTrust's patent claims.

[2] For this reason, InterTrust's lengthy argument that "secure" has a meaning in the art is beside the point. InterTrust Opp., at 2-3. As Microsoft stated in its opening brief, "while communicating a general or conceptual meaning, the term 'secure' lacks any precise, uniform definition to inform a person of skill in the art what it means *unless a number of questions are answered.*" Microsoft's Brief in Support of Motion, at 3 (emphasis added).

> In that process, I have read the claims and have some understanding of what they appear to promise and what they seem to mean in general. But as far as doing further detailed analysis of what is exactly required by each claim, I haven't really studied that in -- in a proper way yet.

Wesenberg Reply Decl., Exh. A (Mitchell Depo., Vol. 2, at 299:1-17).

Because the challenged claims use "secure" without providing specific parameters or criteria or referencing any in the art, one cannot determine their scope by reading them. A person of ordinary skill is left unable to define "secure" in light of the art and thus unable to understand the claims precisely enough to know what is in their scope.

B. <u>The Specification Does Not Select Any Criteria for Evaluating "Secure", Though It Refers to Some</u>

Faced with a vague and general "ordinary" meaning, we look to the patent specifications to see if they point to any of the criteria recognized in the art. InterTrust and Microsoft have identified some of the well-known "off-the-shelf" standards for determining "security," including the Common Criteria for Information Technology Security Evaluation, the Trusted Computer System Evaluation Criteria ("TCSEC"), and Federal Information Processing Standard 140-1 ("FIPS 140-1"). InterTrust Brief, p. 3; Reiter Decl., pp. 3-7. The fatal problem with InterTrust's specifications is that while they mention some of these standards, they adopt none of them. Nowhere is there a clear indication that a particular standard or identified criteria is the one to follow. The specification treats them as optional and applicable, if at all, only to a small part of the universe of the patent.

The TCSEC, for instance is mentioned in one column of the '193 patent, in a discussion of the possible use of VDE to support document management for a large organization. In a list of examples of how "VDE-enforced control capabilities" can be used to manage documents, the specification states that one particular type of document transmission channel and one type of storage device "could be" set up with restrictions that would satisfy the Device Labels requirement of the TCSEC. '193, col. 279:45-60. But these are just two examples (out of nine) of uses to which VDE can supposedly be put in one type of customer context, out of a great many others promised in the patent. Nowhere does the patent state or even suggest that TCSEC or any part of it is meant to provide criteria to define "secure" throughout the patent, and interTrust does not make that argument now.

Likewise, the '721 specification mentions the FIPS-186 "Digital Signature Standard," but only as one possible methodology for evaluating the "security" of a digital signature. Again, InterTrust does not even argue that this is the standard a person of skill should use to evaluate whether something is "secure," but merely that one could do so.

C. <u>The Specification Does Not Define "Secure" for Purposes of the Patent</u>

Lacking a known criteria or a specified new criteria, an otherwise indefinite claim can be saved if the specification defines the proper measure of the problem term. Unfortunately, the 900+ pages of the patent specification point in so many different directions that it is impossible to know which apparent definition of "secure" to use. The patent does contain a great deal of verbiage about security methods and degrees. But its discussion of these issues is tantamount to a recitation of almost everything security could possibly mean or include, including unbounded references to whatever is not expressly recited in the patent.

1. <u>The Specification Does Not Define "Secure" Explicitly</u>

The patent never explicitly defines what "secure" means, either lexically or by outlining its own security policy or set of security criteria, a fact which InterTrust has not disputed.

2. <u>The Specification Does Not Define "Secure" by Functional Description</u>

The specification also fails to give "secure" a precise and unambiguous meaning by describing it functionally. That is, no clear and precise meaning of "secure" can be derived from the technological features disclosed in the specification. Although the specification contains a voluminous recitation of detail, that detail itself describes so many purportedly different levels of "security" that it is impossible to tell which technological features suffice to make a system "secure" in any particular instance. (As discussed below, it is inconsistent for InterTrust to argue that the specification provides the detail needed to make "secure" definite enough to determine what infringes, when it has excluded any such detail from its proposed Markman definition of the same term.)

The discussion of encryption mechanisms cited by InterTrust as supposed evidence of secure's definiteness exemplifies this. InterTrust argues that the '193 patent "contains a passage contrasting 'highly secure' encryption algorithms with 'extremely secure' algorithms, and explicitly identifies each type of algorithm, including explaining circumstances under which each should be used." InterTrust's opposition brief blithely reassures the reader that "both 'highly secure' and 'extremely secure' algorithms are 'secure.'" But these phrases clearly denote different degrees of security. To which level do the claims refer when they employ "secure"? InterTrust's answer that the specification tells one which "secure" mechanisms to use under which circumstances is untrue. The "highly secure" algorithm in this example is described simply as a "'bulk encryption/decryption technique.'" '193, col. 67:18-19. Elsewhere, the patent states that VDE "does not require any specific algorithm ... for bulk encryption/decryption." '193, Col. 201:27-29. More importantly, for both the "highly secure" and "extremely secure" cases, the measures mentioned are described as "preferable." *Id.*, col. 67:18, 21. This implies that there are circumstances under which the "preferable" option would not be employed, raising the question of what those circumstances are, who would make the decision, and how.

The next example cited by InterTrust begins to answer that question: in fact, "secure" is not evaluated by anything intrinsic to the patent, but by a subjective and unpredictable decisionmaking process. A discussion of encryption techniques that InterTrust offers as proof of the specificity with which the patent allegedly endows "secure," InterTrust Opp., at 6; '193, col. 201:63-202:12, is immediately preceded by this explanation:

> VDE 100 provided by the preferred embodiment accommodates and can use many different key lengths. The length of keys used by VDE 100 in the preferred embodiment is determined by the algorithm(s) used for encryption/decryption, ***the level of security desired***, and throughput requirements. Longer keys generally require additional processing power to ensure fast encryption/ decryption response times. Therefore, there is a tradeoff between (a) security, and (b) processing time and/or resources. Since a hardware-based PPE encrypt/decrypt engine 522 may provide faster processing than software-based encryption/decryption, the hardware-based approach may, in general, allow use of longer keys.

'193, Col. 201:50-62. There is no constraint placed on the "level of security desired" – it is up to the user or system designer (or someone – the patent does not say whom) to balance security against their subjectively perceived costs in deciding what key lengths to use. The entire discussion of key lengths that follows is therefore dependent on a preference external to the patent. It is not enough to give technical details about key lengths, because whatever key length a person of skill in the art might choose or encounter fails to answer the question whether the product or activity in question is or isn't "secure" as used in the claims.

III. INTERTRUST'S EFFORTS TO DEFEND "SECURE" REVEAL THE INDEFINITE MEASURE OF SECURITY IMPLICIT IN THE PATENT

InterTrust's proposed solutions to the patent's lack of a standard for "secure" – its Markman definition and or a "commercially reasonability" standard – reveal precisely why the term is indefinite. The evidence confirms that "secure" as used in the claims has no fixed, precise meaning and is constrained by no criteria.

A. The Proposed Markman Definition Is Indefinite

Contrary to its concession of the need for criteria, InterTrust asserts that its proposed *Markman* definition of "secure" is sufficiently definite. InterTrust Opp., at 4. InterTrust's opposition brief omits, however, a crucial sentence within its proposed definition: "Security is not absolute, but designed to be sufficient for a particular purpose." Joint Claim Construction Statement, Exh. A, at 1. The definition states no "purpose," leaving the person of skill in the art completely in the dark as to how much security is needed, or for what, as well as how to measure it.

B. The Proposed Standard of "Commercial Reasonableness" Is Indefinite and Unsupported by the Patent

InterTrust's Opposition brief suggests an alternative definition for "secure" – "commercial reasonability." Having admitted the need for criteria, and challenged to show where the patents provide such criteria, InterTrust asserts that "[t]he information included in the InterTrust patents includes guidance regarding how security should be measured, including the statement that security should be based on a commercially reasonable standard." Opp., 3-4. Dr. Reiter elaborates in his declaration, reiterating the need for context and criteria, but stating that "computer security professionals routinely apply a commercial reasonability standard in building security into real-world products and in determining whether real-world products or processes are 'secure.'" Reiter SJ Decl., at 12, 18.

If the "commercial reasonability" standard were in fact supported by the patent or the evidence, it would still leave the claims indefinite. But the Court need not even consider that question, because InterTrust's expert, Dr. Reiter, admits that the "commercially reasonable" standard referred to in his second Declaration differs from InterTrust's proposed *Markman* definition. When asked if he drafted the above-quoted sentence about computer security professionals "routinely apply[ing] a commercial reasonability standard," Dr. Reiter responded that he had neither drafted nor dictated it, saying only that he "remember[s] discussing issues like this with InterTrust before this was drafted, as far as I know, because I don't actually know when it was drafted." Reiter Depo., 4/17/03, p. 420:1-20 attached to Wesenberg Reply Decl., Exh. B. That led to the following exchange:

> Q: You recall discussing the opinion that computer security professionals routinely apply a commercial reasonability standard with InterTrust before you arrived at InterTrust and were given the draft of this declaration that's been marked as Exhibit 69?
>
> A. Certainly I remember discussing security is meant to be sufficient for a given purpose or a given set of threats and that requirements for commercial systems would be different than for other types of systems. I don't know if I used exactly the words commercial reasonability standard, though.
>
> Q. Do you understand "commercial reasonability standard" to be synonymous with "designed to be sufficient for a particular purpose"?
>
> A. I don't think I would say they're synonymous.
>
> Q. How do they differ?
>
> A. Commercial reasonability indicates a particular type of purpose or, you know, a particular – I should say maybe set of threats to which protection mechanisms should be robust or against which they should be robust.

Reiter Depo., 4/17/03, pp. 420:21-421:22, Wesenberg Reply Decl., Exh. B. "Commercial reasonability" thus not only means something different from InterTrust's proposed Markman definition, it also (unlike InterTrust's proposed Markman definition) gives at least a general indication what kinds of threats the system is to be secured against.

In fact, the commercial reasonability standard appears nowhere in the patent. Tellingly, Dr. Reiter's declaration does not assert that the patent teaches "commercial reasonability" – only InterTrust's brief makes that claim, citing two excerpts from the specification as support. InterTrust Opp., at 4 n.4. But the cited specification language says nothing about how to evaluate or define "reasonability." Rather, it refers to "sufficient security (sufficiently trusted) for the intended commercial purposes" and states that the level of security **depends on "the commercial requirements of particular markets or market niches, and may vary widely."** '193, Col. 45:39-45, 49:59-62 (emphasis added). These statements effectively admit that "secure" is indefinite as used in the claims.

C. InterTrust Has Effectively Admitted that Secure Is Indefinite

The patent language that InterTrust cites as support for the "commercial reasonability" standard acknowledges that in these patents the only criteria of "secure" "depends on the commercial requirements of particular markets or market niches, and may vary widely." '193 patent, Col. 49:61-62, quoted in Joint Claim Construction Statement, Exh. C, item 19(B), 19(J), cited in InterTrust Opp., at 4 n.4. This admits indefiniteness, because no measure or method is identified which would let people of skill in the art precisely and reliably reach the same conclusion whether something is "secure" in those admittedly widely varying markets – especially where each of those markets consists of many different companies and people, and many possible different standards and "requirements."

InterTrust's brazenness in taking this position is apparently a function of its confidence that it can overwhelm Microsoft and the Court by citing to the numbing abundance of technical description in its gargantuan patents. The mere presence of voluminous description of possible technologies does not provide the needed measure.

IV. INTERTRUST COINED TERMS "PROTECTED PROCESSING ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" AS USED IN ITS PATENTS LACK THE NECESSARY DEFINITENESS TO ONE OF ORDINARY SKILL IN THE ART

Like its arguments regarding "security," InterTrust's arguments regarding Protected Processing Environment ("PPE") and Host Processing Environment ("HPE") miss the mark. In its Opposition, InterTrust simply ignores its burden of defining coined terms with "precision." *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F. 3d 1563, 1570 (Fed. Cir. 1997). Instead it argues that HPE and PPE receive "extensive discussion in the specification."

Whatever the extent of the discussion, InterTrust points to no instance where these terms are clearly and ***precisely*** defined. Microsoft's primary contention is that when used, the coined phrases HPE or PPE, are used inconsistently, sometimes contradictorily and nearly always shrouded in qualifying and conditional language. The passages from the '193 specification attached to Dr. Reiter's declaration illustrate these defects. First, the nature of, and relationship between, "SPE", "PPE" and "HPE", is indeterminate. In a passage from the '193 specifications and cited by InterTrust's expert, the following relationship is described:

> ROS 602 in this example also includes one or more Host Event Processing Environment ("HPEs") 655 and/or one or more Secure Event Processing Environments ("SPEs") 503 (these environments may be generically referred to as "Protected Processing Environments" 650). (Col. 79, 30-35)

It can be surmised from this that reference to a PPE could mean either SPE or HPE. The specification, however, identifies that "HPEs" may be provided in two types, "Secure" and "Not Secure," and InterTrust leaves one to guess which is which in any given instance. Indeed, InterTrust admits that its proposed definition of HPE does not acknowledge this schism, yet InterTrust offers only a circularity as a remedy: that non-secure HPEs be defined to be HPEs that are not secure.

Any attempt to distinguish these terms by their structural or functional characteristics is futile. When text is actually committed to discussing a "PPE", "SPE" or "HPE" the qualities and/or attribute assigned each are merely optional. In the text following the introduction of the terms PPE and HPE (Col. 79, 31-35) the specification identifies no fewer than four attributes that "may" be aspects of an SPE or HPE. "HPEs and SPEs are self-contained computing and processing environments that ***may include*** their own operating system kernel, ... ***may process*** information in a secure way, ... they ***may*** each perform ... they ***may*** each offer ...". Reiter Decl., Ex. G., p. 2 (Col. 79, 36-46). (Emphasis added.) As demonstrated in this example, representations about functional and design characteristics of HPE's and PPE's are frequently qualified with the term "may be" or "can be." The first two full paragraphs of Reiter Ex. G at p. 3 when referring to HPEs or SPEs use "may," "may be," "can be" or "could" fifteen times. Every sentence but one does so. The constant use of such qualifying language leaves one irredeemably confused as to the nature and characteristics of the PPEs and HPEs. Again, there is plenty of verbiage directed generally at these terms but they remain undefined, and certainly cannot be understood with anything approximating "precision."

InterTrust's argument that Professor Mitchell "has no difficulty understanding what the term [PPE] means" is both wrong and of no consequence. Microsoft has never disputed that one of ordinary skill in the art would be able to surmise what these coined terms ***might*** suggest when dissected into their component parts. The section of the Mitchell declaration cited by InterTrust is under the caption "what the claim appears to promise." This standard neither purports to, and does not, comport with the requirement of 35 U.S.C. § 112(2).

V. ARGUMENT

A. The Lack of Criteria or Parameters for "Secure" Render It Indefinite

InterTrust's concession that persons of skill in the art require criteria to understand "secure" with any precision, and that there are many different possible sets of criteria, greatly simplifies the analysis in this case. In *Amgen v. Hoechst Marion Roussel, Inc.*, the Federal Circuit held that claim language that could be measured by multiple recognized standards failed for indefiniteness where the written disclosure named several standards but failed to specify which one was to be used. 314 F.3d 1313, 1341-42 (Fed. Cir. 2003). Different methods of purifying human urinary erythropoietin ("uEPO") would produce samples with different glycosylation, which meant that the claim limitation "having glycosylation which differs from that of human uEPO" was a "'moving target.'" *Id.* at 1340, 1341 (quoting lower court). Finding that the specification of the patent "does not direct those of ordinary skill in the art to a standard by which the appropriate comparison can be made," the Court held that "such ambiguity in claim scope is at the heart of the definiteness requirement of 35 U.S.C. § 112 ¶ 2," and affirmed the lower court's finding of indefiniteness. *Id.*, at 1341, 1342. Similarly, the failure of the InterTrust patents to choose from among the many different standards by which "secure" could be measured, or to specify clear criteria of its own, renders the claims containing the term "secure" and its variants indefinite.

B. Indexing a Claim Term to Market Conditions Creates Impermissible Indefiniteness

Instead of providing a standard, InterTrust has adopted the position that "secure" in this patent "depends on the commercial requirements of different markets or market niches, and may vary widely." That 'criterion' is an unpredictable, moving target, much like the claim term in *Ex parte Brummer*, 12 U.S.P.Q.2d 1653 (B.P.A.I. May 11, 1989). The term at issue in that case depended not on any objectively ascertainable feature, but on the label the manufacturer chose to place on the bicycle reflecting its subjective conception of the customer for whom the product was intended. *Id.*, at 1655. InterTrust's argument that this case is more like *Orthokinetics v. Safety Travel Chairs, Inc.*, 806 F.2d 1565 (Fed. Cir. 1986) is fallacious. In *Orthokinetics*, the term that depended on a factor outside the patent was a length parameter – a one-dimensional variable, so to speak. More importantly, it was not subjective. One of ordinary skill in the art building the claimed travel chair "would easily have been able to determine the appropriate dimensions" by measuring the particular automobile. *Id.* at 1576. The Court therefore found it unnecessary to require the claims to list "all possible lengths corresponding to the spaces in hundreds of different automobiles." *Id.* In *Brummer*, no amount of "listing" in the patent could possibly do the trick, because the terms on which the claim scope depended were subjective – the manufacturer's view of whom the bicycle was intended for, and the characteristics of the rider. Similarly, in this case, a person of skill in the art cannot possibly know what a particular customer, market or market niche will deem sufficiently "secure" until after it has sold the product.

Indeed, the fact that one cannot determine the scope of a claim until a product is first manufactured and sold demonstrates that the terms employing "secure" are also indefinite under the principle of *STX, Inc. v. Brine, Inc.*, 37 F. Supp. 2d 740 (D. Md. 1999), *aff'd* on other grounds, 211 F.3d 588 (Fed. Cir. 2000). In that case, subjective claim language describing a lacrosse stick ("improved handling and playing characteristics") would require one to play with the stick in order to determine whether it possessed the limitation and therefore infringed. "The notion that one reasonably skilled in the art would have to infringe the patent claim in order to discern *the boundaries of the claim* is repugnant to long-standing principles of patent jurisprudence." *Id.*, at 755. Here too, one would have to manufacture and sell the product to determine whether it would enjoy market success and would thus have "sufficient security for the intended commercial purposes."

C. "Secure" Must Be Definite Because It Is Essential to VDE

InterTrust assails Microsoft for taking the position that the central importance of "secure" to VDE renders it crucial that the term be sufficiently definite. InterTrust Opp., at 20-21. Contrary to InterTrust's argument, Microsoft did not assert a lower standard of proof of indefiniteness; it sought to foreclose any such argument that InterTrust might make. InterTrust's own reading of *Exxon* confirms that noncritical limitations can sometimes be expressed in functional terms, while critical limitations cannot. Moreover, InterTrust's denial that its expert testified that security is "essential to VDE" is false. InterTrust Opp., at 21-22. Asked about "security," Dr. Reiter answered as follows: "I believe it's an essential aspect of VDE as described in the specification, or in the sense that certainly the authors invest a lot of time on questions of security, and so I think that's probably what they had in mind." Wesenberg Reply Decl., Exh. D (Reiter Depo., 2/28/03, at 23:16-20).[3] "Security" is a critical limitation, and must be sufficiently definite.

D. The Use of "Secure" in Other Patents (and Other Contexts) Is Completely Irrelevant to Whether the Claims at Issue Are Definite

It is a well-known aspect of indefiniteness case law that the same terms are held indefinite in some cases, and definite in others. Thus, the question of whether secure may have been used with sufficient definiteness in other patents, articles, etc., is irrelevant to whether it is sufficiently definite here. In holding that a claim using the term "about" was indefinite, the Federal Circuit warned: "In arriving at this conclusion, we caution that our holding that the term

[3] Microsoft's citation of this statement was off by five lines in the opening brief, the citation starting at line 21 instead of line 16 on the same page.

'about' renders indefinite claims 4 and 6 should not be understood as ruling out any and all uses of this term in patent claims. It may be acceptable in appropriate fact situations, even though it is not here." *Amgen, Inc. v. Chugai Pharmaceutical Co., Ltd.*, 927 F.2d 1200, 1218 (Fed. Cir. 1991). Microsoft has never argued that "secure" cannot be used with sufficient definiteness, only that InterTrust's patents fail to do so. InterTrust's arguments about Microsoft's use of "secure" in its patents are irrelevant, as well as mistaken. (For example, the Slivka '671 patent asserted in this case stands in marked contrast to InterTrust's use of "secure" in the claims at issue on this motion, not least because the Slivka '671 patent sets forth a clear standard by which secure or not secure can be evaluated).

1. The Non-Patent Documents that Employ the Term Are Not Required to Satisfy 35 U.S.C. § 112

Equally irrelevant is InterTrust's argument that "secure" is used in myriad publications and other contexts without the specification of every parameter. Microsoft agrees that "secure" is used in the art in many different ways, some quite vague. That is precisely why it is necessary to specify what is meant when using the term in a patent claim. Patent claims must satisfy 35 U.S.C. § 112(2); the publications InterTrust cites need not. (It is worth noting, however, that the only Microsoft publication provided to the Court by InterTrust uses the Common Criteria to evaluate security – in telling contrast to InterTrust's pervasive failure to identify a definite standard or measure by which "secure" can be evaluated by one of skill in the art. *See* Reiter SJ Decl., Exh. J).

VI. INTERTRUST'S EFFORT TO INCORPORATE BY REFERENCE WAS INEFFECTIVE

Patent Office practice surrounding incorporation by reference attempts to balance 1) the need to provide the public a complete written description of the patent (*see, e.g.*, 35 U.S.C. § 112) with 2) "economy, amplification, or clarity of exposition" achieved by allowing lengthy references to be incorporated by reference into an application under certain circumstances. *Ex parte Schwarze*, 151 USPQ 426 (B.P.A.I. 1966); *see* MPEP § 608.01(p). To meet this balance, the Patent Office has directed that: "essential" material may only be incorporated by reference to an issued U.S. Patent or a published U.S. Patent Application. On the other hand, "nonessential material" may be referred to in a variety of ways. *See* MPEP § 608.01(p). Whether material has been incorporated by reference is a question of law. *Advanced Display Sys., Inc. v. Kent State University*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). InterTrust does not deny that the Big Book material is essential material. The '683, '721, and '861 patents all purport to incorporate the "big book" by reference to the unpublished patent application. For example, the '721 states, "This application is related to commonly assigned copending application Ser. No. 08/388,107 of Ginter et al.... We incorporate by reference, into this application, the entire disclosure of this prior-filed Ginter et al. patent application." (721: 1:7-16; cf. 683: 1:7-23; 861 1:7-11). At the time that the applications leading to the '683, '721, and '861 patents were allowed, InterTrust could have easily complied with the appropriate requirement yet chose not to. Here, the '107 application is the "referenced application." The '107 application, in fact, NEVER issued as a patent – so the examiner had no duty to substitute. It is the duty of the applicant to comply with the 112 requirements. *United Carbon Co. v. Binney & Smith Co.*, 317 U.S. 228 (1942). Accordingly, InterTrust should have either taken one of the two simple options that was open to it. It chose not to. Its effort to incorporation by reference was ineffective.

VII. CONCLUSION

For the reasons set forth above, in Microsoft's opening brief and supporting documents and any argument that may be provided at the hearing, Microsoft respectfully ask this Court to grant its motion and find the mini-*Markman* claims to be invalid.

Dated: April 21, 2003

WILLIAM L. ANTHONY
ERIC L. WESENBERG
KENNETH J. HALPERN
ORRICK, HERRINGTON & SUTCLIFFE LLP

Eric L. Wesenberg
Attorneys for Defendant and Counterclaimant
MICROSOFT CORPORATION

United States District Court
For the Northern District of California

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

_______________________________/

AND COUNTER-ACTION.

_______________________________/

No. C 01-1640 SBA

Consolidated with No. C 02-0647 SBA

ORDER DENYING MOTION FOR PARTIAL SUMMARY JUDGMENT AND CONSTRUING "MINI-MARKMAN" CLAIMS

[Docket No. 229]

Plaintiff's Counsel are directed to serve this order upon all other parties in this action.

This matter comes before the Court for two related proceedings. The first is a "mini-Markman" (limited claim construction) proceeding in which the Court shall construe thirty terms and phrases appearing in twelve claims selected by the parties from the numerous claims at issue in this action. The second is Microsoft's Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness (the "Indefiniteness Motion"). The Court held a claim construction hearing on June 11 and 12, 2003, and heard oral argument on the Indefiniteness Motion on June 12, 2003. Having read and considered the papers submitted, having considered the parties' arguments at the hearings, and being fully informed, the Court DENIES the Indefiniteness Motion and CONSTRUES the disputed terms and phrases as set forth below.

United States District Court
For the Northern District of California

I. BACKGROUND

A. Procedural History

Plaintiff and counterdefendant InterTrust Technologies Corp. ("InterTrust") filed its Complaint in case number C 01-1640 SBA on April 26, 2001, its First Amended Complaint on June 26, 2001, its Second Amended Complaint on July 30, 2001, and its Third Amended Complaint on October 25, 2001. In its Third Amended Complaint InterTrust claimed infringement of seven patents. Defendant and counterclaimant Microsoft Corp. ("Microsoft") filed an answer and counterclaims to the Third Amended Complaint on November 15, 2001, alleging infringement of two of its own patents. The Court subsequently held one of the patents asserted in the Third Amended Complaint not infringed, leaving six patents-in-suit from the Third Amended Complaint.

On February 6, 2002, InterTrust filed a second, separate patent infringement action against Microsoft, No. C 02-0647 SBA, claiming infringement of an additional patent. That second patent infringement action was consolidated with the earlier-commenced action on May 3, 2002.

In an Order filed on October 23, 2002, the Court, <u>inter alia</u>, granted InterTrust leave to amend its complaint. Accordingly, on October 24, 2002, InterTrust filed its Fourth Amended Complaint, claiming infringement of eleven patents (<u>i.e.</u>, it added infringement claims regarding four new patents), one of which was the patent-in-suit in Case No. C 02-0647 SBA. Per the Court's October 23, 2002 Order, Case No. C 02-0647 SBA was automatically dismissed as moot upon the filing of the Fourth Amended Complaint. In an Order filed on November 1, 2002, the Court stayed this action in part, staying all proceedings (including discovery) unrelated to twelve claims selected by the parties and listed in the Order; these claims would be subject to limited <u>Markman</u> and indefiniteness proceedings. On November 7, 2002, Microsoft filed an Answer and Counterclaims to InterTrust's Fourth Amended Complaint, in which it claimed infringement of the same two of its own patents that it had asserted in its previous answer and counterclaims.

Thus, at present, InterTrust has asserted eleven patents that are currently in suit, and Microsoft has asserted two, for a total of thirteen patents-in-suit. These patents are:

InterTrust:	5,892,900	(the "'900 patent")
	5,915,019	(the "'019 patent")
	5,917,912	(the "'912 patent")

United States District Court
For the Northern District of California

	5,920,861	(the "'861 patent")
	5,949,876	(the "'876 patent")
	5,982,891	(the "'891 patent")
	6,112,181	(the "'181 patent")
	6,157,721	(the "'721 patent")
	6,185,683 B1	(the "'683 patent")
	6,253,193 B1	(the "'193 patent")
	6,389,402 B1	(the "'402 patent")
Microsoft:	6,049,671	(the "'671 patent")
	6,256,668	(the "'668 patent")

Both parties have asserted various affirmative defenses to the opposing party's infringement claims, and Microsoft additionally seeks declaratory judgments of non-infringement of InterTrust's asserted patents.

B. The Instant Proceedings

1. Mini-Markman Proceeding

Per the Court's Order of February 24, 2003, and the Court's relevant prior and subsequent Orders, the parties are before the Court for a "mini-Markman" proceeding. The Court is construing thirty terms and phrases from twelve claims jointly selected by the parties from the eleven patents asserted by InterTrust. The parties have asked for one additional item of construction: whether a particular term, "virtual distribution environment," should be read into all of the claims at issue as a limitation.[1] The terms and phrases to be construed have been selected from the following twelve claims (from seven of InterTrust's asserted patents):

1. 193.1[2]
2. 193.11
3. 193.15
4. 193.19
5. 683.2
6. 721.1
7. 721.34
8. 861.58
9. 891.1
10. 900.155
11. 912.8

[1] As discussed infra, there is some disagreement about whether Microsoft is asserting that this term should be read into every claim at issue in this proceeding.

[2] The format "XXX.YYY" indicates the following: XXX is the patent number; YYY is the number of the relevant claim in that patent. This format will be used to identify claims throughout this Order.

12. 912.35

The parties have filed a Patent Local Rule 4-3 Joint Claim Construction and Prehearing Statement Revised in Accordance with the Scope of "Mini-Markman" Hearing Set Forth in the Court's Order Entered 2/24/03 (the "JCCS"), which provides most of the essential information for the Court's construction of the terms and phrases at issue. The parties' competing proposed constructions of the terms and phrases are set out in Exhibits A and B to the JCCS (both exhibits provide the parties' proposed constructions but organize them differently). InterTrust's and Microsoft's identifications of intrinsic and extrinsic evidence are set out in Exhibits C and D, respectively, to the JCCS.

In connection with the mini-Markman hearing the parties have submitted the following briefs: InterTrust has submitted InterTrust's Opening Claim Construction Brief ("InterTrust's Opening Markman Brief") (40 pages in length); Microsoft has submitted Microsoft's Markman Brief (40 pages); and InterTrust has submitted Plaintiff InterTrust Technologies Corporation's Reply Memorandum on Claim Construction ("InterTrust's Reply Markman Brief") (25 pages). The parties have also submitted various declarations with attachments in support of their briefs. On InterTrust's motion, the Court struck the testimony of witnesses David Maier, Sanford Bingham, and Martin Plaehn, offered by Microsoft in support of its claim construction positions, in two Orders filed on June 5 and 10, 2003.

The parties have filed a Joint Appendix to Joint Claim Construction Statement (the "JA"), which consists of a brief cover document and 18 volumes containing the full seven patents-in-suit from which the 12 claims that are the subject of the mini-Markman proceeding are taken (Exhibits A through G), the prosecution histories of these seven patents (Exhibits H through Q), selected cited references (Exhibits R through DD), and a related patent application (Exhibit EE).

2. Indefiniteness Motion

Also per the Court's Order of February 24, 2003, and the Court's relevant prior and subsequent Orders, the parties are before the Court for resolution of Microsoft's Indefiniteness Motion. The Indefiniteness Motion seeks summary judgment on the issue that those of the claims at issue that contain any of the terms "secure," "protected processing environment," or "host processing environment" are invalid as indefinite. These terms are three of the 30 terms to be construed in the mini-Markman proceeding.

The parties' briefing on the Indefiniteness Motion consists of the following: Microsoft's Brief in Support of Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness ("Microsoft's Opening Indefiniteness Brief"); the Memorandum of Points and Authorities of Plaintiff InterTrust Technologies in Opposition to Microsoft (sic) Motion for Summary Judgment on Indefiniteness and in Support of Cross-Motion for Summary Judgment ("InterTrust's Indefiniteness Opposition Brief");[3] and Reply to InterTrust's Opposition to Microsoft's Brief in Support of Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness" ("Microsoft's Reply Indefiniteness Brief"). Both parties' briefs overwhelmingly focus on the term "secure." The parties have also submitted various declarations with attachments in support of their briefs. Of Microsoft's evidentiary submissions, on InterTrust' motion the Court struck the testimony of witnesses Jim McLaughlin, Julien Signes, Damian Saccocio, and Karl Ginter,[4] in an Order filed on June 5, 2003.

II. LEGAL STANDARDS

A. Claim Construction Generally

A patent confers the right to exclude others from making, using, or selling the invention defined by the patent's claims. See Standard Oil Co. v. Am. Cyanamid Co., 774 F.2d 448, 452 (Fed. Cir. 1985). A patent must describe the exact scope of an invention and its manufacture to secure to a patentee all to which he is entitled, and to apprise the public of what is still open to them. See Markman v. Westview Instruments, Inc., 517 U.S. 370, 373, 116 S. Ct. 1384 (1996). These objectives are served by two distinct elements of a patent document. First, it contains a specification

[3] In filing its opposition brief to the Indefiniteness Motion, InterTrust asserted a Cross-motion for Partial Summary Judgment in which InterTrust sought summary judgment on the issue that eleven of the patent claims asserted by InterTrust are definite. In its Order Staying Cross-Motion and Briefing Thereon, filed on April 23, 2003, the Court stayed this cross-motion and all briefing related to the cross-motion until further order of the Court.

[4] Transcripts of these witnesses' testimony are appended to the Declaration of Eric L. Wesenberg in Support of Microsoft Corporation's Motion for Summary Judgment that Certain Mini-Markman Claims Are Indefinite as Exhibits C, D, H, and I, respectively.

describing the invention in such full, clear, concise, and exact terms as to enable any person skilled in the art to make and use the same. See 35 U.S.C. § 112. Second, a patent includes one or more claims, which particularly point out and distinctly claim the subject matter which the applicant regards as his or her invention. See id.

The first step in any invalidity or infringement analysis is claim construction. See Union Oil Co. v. Atl. Richfield Co., 208 F.3d 989, 995 (Fed. Cir. 2000). The construction of claims is simply a way of elaborating the normally terse claim language in order to understand and explain, but not to change, the scope of the claims. See id. Claim construction is a matter of law to be determined by the court. See Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995), aff'd, 517 U.S. 370, 116 S.Ct. 1384 (1996).

B. Consideration of Evidence in Connection with Claim Construction

1. Intrinsic Evidence

"It is well-settled that, in interpreting an asserted claim, the court should look first to the intrinsic evidence of record, i.e., the patent itself, including the claims, the specification, and, if in evidence, the prosecution history." Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996) (citing Markman, 52 F.3d at 979). In the context of the intrinsic evidence, the court should first look to the language of the claims themselves. See id. Words in a claim are generally given their ordinary and customary meaning as understood by one of ordinary skill in the art. See id.; see also Dow Chem. Co. v. Sumitoro Chem. Co., 257 F.3d 1364, 1373 (Fed. Cir. 2001) ("[A] technical term used in a patent claim is interpreted as having the meaning a person of ordinary skill in the field of invention would understand it to mean."). It is well-established that "dictionaries, encyclopedias and treatises are particularly useful resources to assist the court in determining the ordinary and customary meanings of claim terms." Tex. Digital Sys., Inc. v. Telegenix, Inc., 305 F.3d 1193, 1202 (Fed. Cir. 2002); see also Dow Chem., 257 F.3d at 1373 ("Dictionaries and technical treatises . . . hold a special place and may sometimes be considered along with the intrinsic evidence when determining the ordinary meaning of claim terms.").[5] A dictionary definition may not be relied on, however, if it contradicts any definition found in or ascertained by a reading of the patent documents. See Kopykake Enters., Inc. v. Lucks Co., 264 F.3d 1377, 1382 (Fed. Cir. 2001) (citing Vitronics, 90 F.3d at 1584 n.6). The Court should rely on specialized, technical dictionaries that reflect the understanding of one skilled in the art, rather than lay dictionaries. AFG Indus. v. Cardinal, 239 F.3d 1239, 1247–48 (Fed. Cir. 2001) ("Dictionary definitions of ordinary words are rarely dispositive of their meanings in a technological context.") (citing Anderson v. Int'l Eng'g & Mfg., Inc., 160 F.3d 1345, 1348–49 (Fed. Cir. 1998); see also Hoescht Celanese Corp. v. BP Chems. Ltd., 78 F.3d 1575, 1580 (Fed. Cir. 1996)).

"Although words in a claim are generally given their ordinary and customary meaning, a patentee may choose to be his own lexicographer and use terms in a manner other than their ordinary meaning, provided the special definition of the term is clearly stated in the specification." Vitronics, 90 F.3d at 1582. Therefore, it is necessary to review the specification to determine whether the patentee has used terms inconsistent with their ordinary and customary meaning. See id.; see also Dow Chem., 257 F.3d at 1373 ("[T]he court must examine the intrinsic evidence to determine whether the patentee has given a term an unconventional meaning."). Thus, the specification acts as a dictionary when it expressly defines a term used in the claim or defines it by implication. See Vitronics, 90 F.3d at 1582 (citing Markman, 52 F.3d at 979). However, in examining the specification, the court must not read limitations from the specification into the claims. See Burke, Inc. v. Bruno Indep. Living Aids, Inc., 183 F.3d 1334, 1340 (Fed Cir. 1999); Comark Communications, Inc. v. Harris Corp., 145 F.3d 1182, 1186–87 (Fed. Cir. 1998) (limitations from specification are not to be read into the claims, but there is a fine line between reading a claim in light of the specification and reading a limitation into the claim from the specification); but see Scimed Life Sys., Inc. v. Advanced Cardiovascular Sys., 242 F.3d 1337, 1341 (Fed. Cir. 2001)

[5] Although such materials have regularly been characterized as extrinsic evidence, albeit special extrinsic evidence that may be considered along with intrinsic evidence, e.g., Dow Chem., 257 F.3d at 1373, the Federal Circuit has cautioned that "categorizing them as 'extrinsic evidence' or even a 'special form of extrinsic evidence' is misplaced and does not inform the analysis." Tex. Digital, 305 F.3d at 1203.

("Where the specification makes clear that the invention does not include a particular feature, that feature is deemed to be outside the reach of the claims of the patent, even though the language of the claims, read without reference to the specification, might be considered broad enough to encompass the feature in question.").

Finally, if it is entered into evidence, the court must examine the prosecution history of the patent. See Dow Chem., 257 F.3d at 1373; Vitronics, 90 F.3d at 1582. The prosecution history contains the complete record of the proceedings before the Patent and Trademark Office, and may include express representations made by the applicant regarding the scope of the claims. See Vitronics, 90 F.3d at 1582. The court examines the prosecution history to determine "whether the patentee has 'relinquished a potential claim construction in an amendment to the claim or in an argument to overcome or distinguish a reference.'" Dow Chem., 257 F.3d at 1373 (citing Interactive Gift Exp., Inc. v. Compuserve Inc., 256 F.3d 1323, 1331 (Fed. Cir. 2001)); see also Pall Corp. v. PTI Technologies Inc., 259 F.3d 1383, 1392 (Fed. Cir. 2001) ("[I]t is well established that '[t]he prosecution history limits the interpretation of claim terms so as to exclude any interpretation that was disclaimed during prosecution.'") (citing Southwall Technologies, Inc. v. Cardinal IG Co., 54 F.3d 1570, 1576 (Fed. Cir. 1995)). A narrower claim interpretation will be adopted if the "accused infringer can demonstrate that the patentee 'defined' the claim as 'excluding' a broader interpretation 'with reasonable clarity and deliberateness.'" Pall Corp., 259 F.3d at 1393 (citing N. Telecom Ltd. v. Samsung Elecs. Co., 215 F.3d 1281, 1294–95 (Fed. Cir. 2000)).

2. Extrinsic Evidence

In most cases, an examination of the intrinsic evidence will be sufficient to resolve any ambiguity in the disputed claim and it would be improper to rely on extrinsic evidence. See Vitronics, 90 F.3d at 1583 (citing Pall Corp. v. Micron Separations, Inc., 66 F.3d 1211, 1216 (Fed. Cir. 1995)). Extrinsic evidence may be used to define the claim only if the claim language remains "genuinely ambiguous" after consideration of the intrinsic evidence. See id. However, "it is entirely appropriate, perhaps even preferable, for a court to consult trustworthy extrinsic evidence to ensure that the claim constructions it is tending to from the patent file is not inconsistent with clearly expressed, plainly apposite, and widely held understandings in the pertinent technical field.'" AFG

Indus., 239 F.3d at 1249 (quoting Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1309 (Fed. Cir. 1999)); see also Bell v. Howell Document Mgmt. Prods. Co., 132 F.3d 701, 706 (Fed. Cir. 1998); Mantech Envtl. Corp. v. Hudson Envtl. Servs., Inc., 152 F.3d 1368, 1373 (Fed. Cir. 1998).

> When "the specification explains and defines a term used in the claims, without ambiguity or incompleteness, there is no need to search further for the meaning of the term." However, when such definition is challenged it is often appropriate, despite facial clarity and sufficiency of the specification and the prosecution history, to receive evidence of the meaning and usage of terms of art from persons experienced in the field of the invention.

ATD Corp. v. Lydall, Inc., 159 F.3d 534, 540 (Fed. Cir. 1998) (citations omitted). A court may hear all relevant testimony—including expert testimony—so long as it does not accord weight to expert testimony that contradicts the clear language of the claim. See Vitronics, 90 F.3d at 1584.

C. **Invalidity Based on Indefiniteness**

A patent is presumed to be valid. 35 U.S.C. § 282. A party challenging the validity of a patent must prove the invalidity by clear and convincing evidence. See Apotex USA, Inc. v. Merck & Co., 254 F.3d 1031, 1036 (Fed. Cir. 2001); Loral Fairchild Corp. v. Matsushita Elec. Indus. Co., 266 F.3d 1358, 1361 (Fed. Cir. 2001).

A patent claim satisfies the definiteness requirement of paragraph 2 of 35 U.S.C. § 112 only if "one skilled in the art would understand the bounds of the claim when read in light of the specification." Exxon Research & Eng'g Co. v. United States, 265 F.3d 1371, 1375 (Fed. Cir. 2001) (citing Miles Labs., Inc. v. Shandon, Inc., 997 F.2d 870, 875 (Fed. Cir. 1993)). This means that the claims at issue must be "sufficiently precise to permit a potential competitor to determine whether or not he is infringing." Morton Int'l, Inc. v. Cardinal Chem. Co., 5 F.3d 1464, 1470 (Fed. Cir. 1993). But a claim is not indefinite "merely because it poses a difficult issue of claim construction"; the claim need only "be amenable to construction, however difficult that task may be." Exxon Research, 265 F.3d at 1375. Whether a claim is indefinite is a question of law. Id. at 1376.[6]

[6] In Microsoft's Opening Indefiniteness Brief, Microsoft claims that the determination of definiteness involves application of a two-part test. (Microsoft's Opening Indefiniteness Br. at 21.) InterTrust disputes the validity of this test, arguing that the Federal Circuit has clearly rejected the requirement, asserted by Microsoft, that claims be drafted as precisely or specifically as possible. (InterTrust's Indefiniteness Opp. Br. at 15 (quoting PPG Indus., Inc. v. Guardian Indus. Corp., 156 F.3d

III. DISCUSSION

As an initial matter, the Court notes that the relevant "art" of the claims at issue in the mini-Markman proceeding and the Indefiniteness Motion is computer security. The Court previously reached this conclusion in its Order re: Unresolved Portion of InterTrust's Motion to Strike Markman Matter after considering supplemental briefing on this issue, and the Court now incorporates by reference its reasoning therein.[7]

The Court addresses the Indefiniteness Motion first for a practical reason: if any of the terms at issue are found indefinite, there would be no need to construe any claim that contains such term or terms.

A. Indefiniteness Motion

Microsoft's Indefiniteness Motion seeks summary judgment on the issue of whether the claims at issue are indefinite with regard to three terms: "secure"; "protected processing environment"; and "host processing environment." The overwhelming majority of the briefing, however, is addressed solely to the term secure. These terms are discussed in turn.

1. Secure

Although Microsoft's discussion of why the term secure is indefinite is lengthy both in its opening brief and its reply brief, the essence of its theory of indefiniteness is a ten-variable test created by Microsoft's expert, Professor John C. Mitchell ("Prof. Mitchell"), which, he contends, is

1351, 1355 (Fed. Cir. 1998), and Exxon Research, 265 F.3d at 1376, 1383–84).)

The Court agrees with InterTrust that Microsoft's asserted two-part test has no basis in law. The principles set forth above in this section of the Order are what govern consideration of Microsoft's Indefiniteness Motion. Microsoft's counsel was prudent to retreat from this alleged two-part test at oral argument, (see Transcript of Proceedings, Claims Construction Hearing ("Tr.") 305:24–306:13), although Microsoft should not have advanced it in the first place.

[7] The Court needs not and does not define what experience or qualifications one must have to be a "person of ordinary skill in the art" of computer security. The Court already struck the testimony of certain of Microsoft's witnesses in its Order re: InterTrust's Motions to Strike on the ground that there was insufficient evidence that they had sufficient skill even under Microsoft's lenient standard of "ordinary skill." None of the remaining testimony tendered by the parties would be subject to exclusion on the ground that the declarant lacked sufficient skill to be competent to testify. Thus, the Court concludes that all remaining witnesses providing testimony regarding the proper construction of the terms and phrases in dispute, particularly Dr. Michael Reiter and Professor John C. Mitchell, have at least the ordinary skill in the art, and the Court evaluates the evidence accordingly.

not satisfied with respect to secure. Specifically, Prof. Mitchell asserts that in order for persons of ordinary skill in the art to understand what is meant by the term secure, they must be able to reach a common understanding with regard to each of the following variables:

1. Protecting what types of things or actions?
2. Protecting what specific things or actions?
3. Protecting what properties of these things or actions (e.g., secrecy/confidentiality, integrity, availability, authenticity, and non-repudiation)?
4. Protecting against whom?
5. Protecting against what points of attack?
6. Protecting against what kind of attacks?
7. Secure for how long?
8. How to test or infer the existence of the protection?
9. What degree of protection?
10. Secure to whom?

(Decl. of Professor John C. Mitchell at 9–11.) Prof. Mitchell's Declaration presents numerous excerpts from the relevant specifications that, he evidently believes, do not allow persons of ordinary skill in the art to reach common understandings regarding any or all of these variables. (See, e.g., id. at 12–18.) Given that the Court has stricken the testimony of witnesses Signes, McLaughlin, Saccocio, and Ginter, Prof. Mitchell's testimony constitutes virtually the entirety of the evidentiary support, other than the text of the claims and specifications themselves, for Microsoft's positions in the Indefiniteness Motion.

InterTrust advances a number of arguments in response to Microsoft's contentions. First, it points out that Prof. Mitchell testified that secure has a general meaning in the field of computer science, and he himself was able to explain his use of the word secure. (InterTrust's Indefiniteness Opp. Br. at 4.) Prof. Mitchell also testified that there is a recognized set of criteria for determining whether a system is secure. (Id. at 5.) Second, InterTrust asserts that the claims of the patents-in-suit use secure in context, placing qualifiers around it that make clear to what they are referring. (Id. at 5–7.) Third, InterTrust notes that Prof. Mitchell's ten-variable test was created for the purposes of litigation and that Prof. Mitchell does not apply this test to any other document; indeed, as InterTrust's expert, Dr. Michael Reiter ("Dr. Reiter"), testifies, Microsoft's own patents and Prof. Mitchell's own computer security papers fail the test. (Id. at 8.) Relatedly, InterTrust provides various examples in which Prof. Mitchell appears to understand what secure means in context, yet he nevertheless finds the term indefinite because it fails to meet his ten-variable test. (Id. at 8–9.)

Fourth, InterTrust, emphasizing that Microsoft must produce clear and convincing evidence, describes the relevant standard for determining indefiniteness, noting that the use of general terms to describe a range of circumstances does not render claims indefinite and that the fact that reasonable persons might disagree regarding the scope of claims does not render them indefinite. (Id. at 10–14.) InterTrust adds that Microsoft's assertion that 35 U.S.C. § 112 requires claims to be drafted "as precisely or specifically as possible" to be definite has been expressly rejected by the Federal Circuit in PPG Industries, Inc. v. Guardian Industries Corp., 156 F.3d 1351 (Fed. Cir. 1998). (Id. at 15.) Fifth, InterTrust notes that the terms secure and securely are used in other patents, including Microsoft's patents. (Id. at 17.) Sixth, InterTrust explains that the Patent and Trademark Office ("PTO") examiners assigned to the InterTrust applications had no difficulty applying the disputed terms to the prior art. (Id. at 18.) Seventh, InterTrust contends that Prof. Mitchell's analysis should be discarded because he made no attempt to construe the claims as a whole, but rather focused on secure in isolation. (Id. at 18–19.) Eighth, InterTrust seeks to distinguish the cases offered by Microsoft in which certain claim terms were held indefinite on the basis that those cases concerned patent applications, not issued patents; in the former there is no presumption of validity, whereas there is such a presumption for the latter. (Id. at 20–22.)

In its reply brief, Microsoft addresses several of InterTrust's arguments. Of particular note is Microsoft's argument that certain patent language defines secure with reference to a particular purpose, but that purpose is not explicitly defined (e.g., commercial requirements), thereby leaving the reader in the dark about the scope of the claim. (Microsoft's Indefiniteness Reply Br. at 7–9, 11–12.) In particular, Microsoft argues that to the extent that secure is defined with reference to the context of the invention's commercial embodiments, it is indefinite. (Id. at 12–13.)[8] In addition,

[8] Related to but independent of the foregoing, Microsoft contends that the effort to incorporate by reference the "Big Book" patent application filed in or about 1995 with respect to the '683, '721, and '861 patents failed because these patents reference the number of the Big Book application, which did not result in an issued patent and therefore was not published. (See Microsoft's Indefiniteness Opening Br. at 12; Microsoft's Indefiniteness Reply Br. at 14–15.) Microsoft contends that "essential" material such as this may be incorporated in a patent only by reference to an issued U.S. Patent or a published U.S. Patent Application. (Microsoft's Indefiniteness Opening Br. at 12.) Microsoft appears to be relying exclusively on § 608.01(p) of the Manual of Patent Examining Procedure (the "MPEP"). (Id.)

United States District Court
For the Northern District of California

Microsoft, quoting deposition testimony of Prof. Mitchell, disputes InterTrust's contention that Prof. Mitchell did not attempt to understand claim terms in the context of the claims. (Id. at 3–4.)

At first blush, Microsoft's arguments and examples are appealing: when read in isolation, many of the claims' uses of the term secure superficially appear ambiguous. But InterTrust has made a convincing case that Microsoft's arguments must be rejected. Perhaps most crucially, the Court agrees with InterTrust that Prof. Mitchell's test is not credible. Prof. Mitchell's test is so unusual and unsupported—probably because, as he admitted, it was created for this litigation—that the Court finds it not credible. There is no evidence whatever, other than Prof. Mitchell's self-serving assertion, that a person of ordinary skill in the art would require definition of all ten variables in the test to understand what is meant by secure. Still further, Prof. Mitchell's opinions are suspect because his declaration does not reflect that he has made any effort to understand the meaning of secure in the context of the claims in their entirety, his deposition testimony on this point

InterTrust disagrees with Microsoft's argument about incorporation by reference. InterTrust contends that there was merely a clerical error. (InterTrust's Indefiniteness Opp. Br. at 23–24.) InterTrust continues that incorporation by reference is effective if the referenced material is reasonably available to the public, and because, according to the MPEP, pending or abandoned applications are readily available to the public from the Patent Office, the Big Book patent application was effectively incorporated. (Id. at 24–25.) InterTrust further argues that MPEP § 608.01(p) requires only that the examiner is supposed to replace an application number with the issued patent number; it does not hold that a patent does not successfully incorporate by reference the material in question if the examiner fails to do so. (Id. at 25.)

The Court finds Microsoft's argument unpersuasive. Microsoft has made no effort to explain how the MPEP constitutes binding authority. To the contrary, the Foreward of the MPEP, of which the Court takes judicial notice, describes the purpose of the MPEP in part as follows:

> This Manual is published to provide U.S. Patent and Trademark Office patent examiners, applicants, attorneys, agents, and representatives of applicants with a reference work on the practices and procedures relative to the prosecution of patent applications before the U.S. Patent and Trademark Office. It contains instructions to examiners, as well as other material in the nature of information and interpretation, and outlines the current procedures which the examiners are required or authorized to follow in appropriate cases in the normal examination of a patent application. The Manual does not have the force of law or the force of the rules in Title 37 of the Code of Federal Regulations.

United States Patent & Trademark Office, Manual of Patent Examining Procedure (Rev. 1, Feb. 2003), available at http://www.uspto.gov/web/offices/pac/mpep/mpep_e8r1_front.pdf (emphasis added). Moreover, the Court has reviewed MPEP § 608.01(p), and the Court agrees with InterTrust that that provision appears only to indicate that the patent examiner should replace an application number with the issued patent number. Accordingly, the Court cannot conclude that the error at issue has resulted in the nonincorporation of the Big Book application by reference.

notwithstanding. Such an approach is not consistent with proper claim construction, which requires interpretation of each claim as a whole. Prof. Mitchell's conspicuous failure to apply his test to the use of the word in other documents suggests that the test has been generated for selective application to InterTrust's patents. And even more damaging to the test's credibility is Dr. Reiter's testimony that application of this test to Microsoft's own patents renders them indefinite.[9] The need to satisfy this test thus seems more hypothetical than real.

Further, as InterTrust correctly points out, the mere fact that persons skilled in the art might disagree about the scope of the claims at issue does not render them indefinite. As the Federal Circuit has observed, "It may of course occur that persons experienced in a technologic field will have divergent opinions as to the meaning of a term, particularly as narrow distinctions are drawn by the parties or warranted by the technology. . . . But the fact that the parties disagree about claim scope does not of itself render the claim invalid." Verve, LLC v. Crane Cams, Inc., 311 F.2d 1116, 1120 (Fed. Cir. 2002).

Nor are the claims at issue indefinite because they use a term that requires an evaluation of the context in which it is used or describes a range of circumstances. On this score the Federal Circuit's reasoning and holding in Orthokinetics, Inc. v. Safety Travel Chairs, Inc., 806 F.2d 1565 (Fed. Cir. 1986), discussed by InterTrust in its opposition brief and at the hearing, demonstrate that Microsoft's concerns are overstated. In Orthokinetics, the Federal Circuit considered whether the term "so dimensioned" from the following claim language was indefinite: "In a wheel chair having a seat portion, a front leg portion, and a rear wheel assembly, the improvement wherein said front leg portion is so dimensioned as to be insertable through the space between the doorframe of an

[9] Microsoft does not respond in its reply brief to Dr. Reiter's testimony about how application of Prof. Mitchell's ten-variable test to several of Microsoft's own patents renders them indefinite. (Microsoft's counsel's assertion at oral argument that Microsoft did address this point in its reply brief, (Tr. 307:15–23), is inaccurate.) At oral argument, however, Microsoft's counsel sought to refute this testimony by arguing that the '671 patent (one of the two patents asserted by Microsoft) expressly defines something to be "secure" as when it is digitally signed. (Tr. 287:22–288:3.) Whatever the merits of this argument, it does not contradict Dr. Reiter's testimony that five other patents held by Microsoft would be indefinite if Prof. Mitchell's test were applied to them. (Decl. of Dr. Michael Reiter in Opp. to Indefiniteness Mot. and in Supp. of InterTrust's Cross-Motion for Summ. J. Ex. D, cited in InterTrust's Indefiniteness Opp. Br. at 8.) The significance of this testimony is that it undermines the credibility of Prof. Mitchell's ten-variable test as representing the perspective of a person of ordinary skill in the art of computer security.

automobile and one of the seats thereof . . . ." Id. at 1568 (emphasis added). The district court had concluded that "so dimensioned" was indefinite because a potential competitor would have to construct a model of a travel chair and test the model on a variety of automobiles before the competitor could determine whether it infringed the patent. See id. at 1575. The Federal Circuit reversed, reasoning:

> It is undisputed that the claims require that one desiring to build and use a travel chair must measure the space between the selected automobile's doorframe and its seat and then dimension the front legs of the travel chair so they will fit in that particular space in that particular automobile. Orthokinetics' witnesses, who were skilled in the art, testified that such a task is evident from the specification and that one of ordinary skill in the art would easily have been able to determine the appropriate dimensions. . . . [¶] That a particular chair on which the claims read may fit within some automobiles and not others is of no moment. The phrase "so dimensioned" is as accurate as the subject matter permits, automobiles being of various sizes. As long as those of ordinary skill in the art realized that the dimensions could be easily obtained, [35 U.S.C.] § 112, 2d ¶ requires nothing more. The patent law does not require that all possible lengths corresponding to the spaces in hundreds of different automobiles be listed in the patent, let alone that they be listed in the claims.

Id. at 1576 (citations omitted).

Similarly, Microsoft has failed to demonstrate that a person of ordinary skill in the art would be unable to determine from the language of the claims and the specifications whether a device might be secure in a sense contemplated by the claims at issue. For example, Microsoft, citing STX, Inc. v. Brine, Inc., 37 F. Supp. 2d 740 (D. Md. 1999), aff'd on other grounds, 211 F.3d 588 (Fed. Cir. 2000), contends that secure is indefinite to the extent that it is defined with reference to the commercial purpose for which it is intended to be used. (Microsoft's Indefiniteness Reply Br. at 12.) Microsoft argues that if one of ordinary skill in the art would have to infringe the patent claim to discern the boundaries of the claim, the claim must be indefinite. (Id. at 12–13.)

The Court agrees with the general proposition that Microsoft advances. But Microsoft, which bears a heavy burden to demonstrate indefiniteness, has failed to offer sufficient evidence that a person of ordinary skill in the art could not discern what would be considered "secure" for a given commercial purpose. Its unsupported assertion in its reply brief that "a person of skill in the art cannot possibly know what a particular customer, market or market niche will deem sufficiently 'secure' until after it has sold the product," (id. at 12), is no substitute for evidence to this effect. Nor is its effort to distinguish Orthokinetics availing: That Orthokinetics involved measurement of a "one-dimensional variable," namely length, (see id.), does not demonstrate that persons of ordinary skill in the art of computer security cannot effectively "measure" several variables. In addition, the fact that "secure" is subjective, in contrast to the clearly objective variable of length, (see id.), does not mean that a person of ordinary skill in the art cannot determine whether or not something is secure within the context that the term is used. The Court is also unaware of any principle in patent law that all operative claim terms must be measurable by some objective standard, and Microsoft does not advance any authority in support of such principle. In sum, it is not self-evident that potential designers of computer security systems are incapable of accurately assessing the commercial purposes for which their systems would be utilized to determine whether these systems are secure within the meaning of the claims at issue and, therefore, whether they infringe them. In the absence of clear and convincing evidence that a person of ordinary skill in the art would be unable to perform this task successfully, the Court cannot conclude that the claims at issue are indefinite.

Were Microsoft not to bear the burden of proving indefiniteness by a clear-and-convincing evidentiary standard, resolution of the Indefiniteness Motion might present a closer call. But such is not the case here. There is no clear and convincing evidence that InterTrust's claims are invalid as indefinite to the extent they contain the term secure. The Court thus DENIES the Indefiniteness Motion with regard to the term secure.

2. Protected Processing Environment (PPE) and Host Processing Environment (HPE)

Microsoft contends that the terms protected processing environment ("PPE") and host processing environment ("HPE") do not have an ordinary or customary meaning inside or outside of the computing world. (Microsoft's Indefiniteness Opening Br. at 15.) Microsoft notes that InterTrust's expert Dr. Reiter testified that a person of ordinary skill in the art would not know what these terms meant in 1995. (Id. at 16.) Citing J.T. Eaton & Co. v. Atlantic Paste & Glue Co., 106 F.3d 1563, 1570 (Fed. Cir. 1997), Microsoft contends that because a person of ordinary skill in the art would not understand these terms, it was InterTrust's duty to supply a precise meaning for these terms. (Id. at 15; see also Microsoft's Indefiniteness Reply Br. at 10.) Microsoft asserts that neither the claims nor the specification provides sufficient description of PPE or HPE to inform a person of ordinary skill in the art what these terms mean. (Microsoft's Indefiniteness Opening Br. at 16–19.)

InterTrust responds that, with regard to PPE, the specification provides detailed descriptions of the key terms on which PPE is based (i.e., secure processing environment ("SPE") and HPE), and therefore PPE is sufficiently defined. (See InterTrust's Indefiniteness Opp. Br. at 22.) InterTrust also points to the various figures in the specification, spread out over dozens of pages, that relate to PPE. (Id.) InterTrust further cites to the Declaration of Dr. Michael Reiter in Opposition to Microsoft's Motion for Summary Judgment and in Support of InterTrust's Cross-Motion for Summary Judgment (the "Reiter Indefiniteness Declaration"), which provides excerpts from the relevant specifications. (Id. (citing Reiter Indefiniteness Decl. ¶¶ 39–40, Ex. G).) Finally, InterTrust rejects Prof. Mitchell's finding PPE indefinite based on application of his ten-variable test. (Id.) As for HPE, InterTrust contends that Microsoft has disingenuously claimed an absence of description in the specification: InterTrust asserts that the terms host processing environment and HPE are used interchangeably; even though the term host processing environment does not frequently appear in the specification, HPE does, along with extensive descriptions. (Id. at 23.)

The potential indefiniteness of these two terms was not addressed at the mini-Markman hearing, but the Court is comfortable resolving the issue on the papers. At the outset, Microsoft's citation to J.T. Eaton & Co. v. Atlantic Paste & Glue Co., 106 F.3d 1563, 1570 (Fed. Cir. 1997), is inapposite. J.T. Eaton has nothing to do with invalidity for indefiniteness, and the cited portion describes merely the patent applicant's obligation to define a coined term precisely in prosecuting its application. See id. at 1568, 1570. Perhaps under J.T. Eaton InterTrust was required to define PPE and HPE when it was prosecuting its applications for the patents-in-suit, but the Federal Circuit's holding therein does not alter Microsoft's burden to provide clear and convincing evidence of indefiniteness.

Microsoft has failed to carry that burden with regard to PPE and HPE. Microsoft itself recognizes that PPE is described to be an SPE and/or an HPE. (Microsoft's Indefiniteness Opening

Br. at 19 (quoting '193 patent at 105:18–21).)[10] Contrary to Microsoft's assertion, this definition by reference is not inherently an unhelpful exercise; it is fruitless only if the incorporated terms are themselves indefinite. Since Microsoft does not contest the clarity or definiteness of SPE, the Court examines only the definiteness of HPE. The Court discusses the proper construction of HPE <u>infra,</u> but in the meantime, it is sufficient for the Court to conclude that Microsoft has failed to provide clear and convincing evidence of indefiniteness. Microsoft's evidence pertaining to HPE, aside from evidence that HPE did not have a meaning known by a person of ordinary skill in the art, consists essentially of a few references to the '900 patent specification. (<u>Id.</u>)[11] But the Court agrees with InterTrust that the description of HPEs in the portion of the '193 patent specification that it cites, ('193 patent at 79:23–83:9), as well as the various figures referenced therein, (<u>e.g.,</u> '193 patent Fig. 10), provide sufficient meaning to the term HPE to survive an indefiniteness challenge.

Were InterTrust now applying for the relevant patents-in-suit, and were the Court the PTO, the Court might require InterTrust to provide greater precision in defining PPE and HPE. But the parties are now before the Court on Microsoft's challenge to the relevant claims' validity, and thus Microsoft bears a heavy burden if its motion is to succeed. In presenting its arguments regarding PPE and HPE, Microsoft appears inclined to shift the burden to InterTrust to defend the validity of its claims. But the burden remains with Microsoft, and Microsoft has failed to put forward sufficient evidence to carry its burden. Accordingly, the Court DENIES the Indefiniteness Motion with regard to the terms PPE and HPE.

///

///

///

[10] Microsoft evidently considers this definition problematic: "This [definition] invariably leaves the relevant public guessing at what might infringe." (<u>Id.</u>) The Court disagrees. Obviously, if PPE is defined to include both SPEs and HPEs, for any embodiment that includes an SPE and/or an HPE and that has other features on which the relevant claim limitations read, the relevant claim is infringed. Thus, for example, the element in 683.2 that provides in part, "a protected processing environment at least in part protecting information . . ." encompasses SPEs and/or HPEs; the public need not guess <u>between</u> SPEs and HPEs, because PPE is defined to include <u>both</u>.

[11] The Court previously struck the testimony of Envivio's and America Online's corporate designees, cited by Microsoft in its Indefiniteness Opening Brief.

B. Construction of Claims at Issue

1. Terms and Phrases for Which Microsoft Did Not Brief Its Position

Out of the thirty terms and phrases selected by the parties for construction, Microsoft elected not to present any argument in its 40-page Markman brief in support of its positions or in opposition to InterTrust's positions on thirteen terms and phrases. These terms and phrases, along with the claims in which they appear, are:

1. aspect (683.2, 861.58, 900.155, 912.8)
2. authentication (193.15)
3. budget (193.1)
4. clearinghouse (193.19)
5. compares (900.155)
6. derive (900.155)
7. designating (721.1)
8. device class (721.1)
9. digital signature/digitally signing (721.1)
10. digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class (721.1)
11. executable programming/executable (721.34, 912.8, 912.35)
12. identifying at least one aspect of an execution space required for use and/or execution of the load module (912.8)
13. securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item (891.1)

At the mini-Markman hearing the Court stated its disinclination to hear oral argument regarding any of these thirteen terms and phrases. The Court reasonably concluded that Microsoft made a decision not to dispute or oppose InterTrust's proposed constructions of these terms and phrases given (1) the number of terms Microsoft declined to address; (2) the importance of written argumentation for the mini-Markman proceeding; and (3) the fact that InterTrust did address every term and phrase at issue.[12]

The Court has reviewed all of InterTrust's briefing on these terms and phrases and finds InterTrust's arguments in support of its relevant positions sound and persuasive. In light of this finding, and given the absence of argument for Microsoft's positions, the Court now adopts InterTrust's proposed constructions for all thirteen of these terms and phrases, other than "budget" and "securely applying . . . said data item."[13]

Aside from the Court's adoption of InterTrust's proposed constructions, the Court wishes to make clear that Microsoft's failure to brief these terms and phrases has serious implications. Microsoft has chosen to dispute these terms and phrases, and it has supplied the Court with proposed constructions. In so doing, Microsoft's attorneys are bound to comply with Rule 11(b), which provides in pertinent part:

> By presenting to the court (whether by signing, filing, submitting, or later advocating) a pleading, written motion, or other paper, an attorney or unrepresented party is certifying that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances, . . . [¶] the allegations and other factual contentions have evidentiary support or, if specifically so identified, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery . . . .

Fed. R. Civ. P. 11(b). Thus, by asserting that the terms and phrases at issue should be defined as proposed by Microsoft, Microsoft's attorneys are representing to the Court that these terms and phrases have evidentiary support. Microsoft's failure now to provide any discussion whatever on these terms and phrases in its Markman brief arguably suggests that Microsoft's attorneys never had

[12] Microsoft has no excuse for failing to provide briefing on these terms and phrases. That InterTrust was able to present in its Markman brief cogent arguments on all thirty terms and phrases, as well as the global construction of "virtual distribution environment," see infra, demonstrates that the 40 pages that the Court granted Microsoft to brief its positions were sufficient to address all terms and phrases in dispute.

[13] The Court excepts these two terms and phrases because Microsoft did brief terms and phrases closely related to these two terms, namely the phrase "a budget specifying the number of copies which can be made of said digital file" and the term "secure."

sufficient factual basis on which to dispute InterTrust's proposed constructions and to offer their own constructions.

The Court takes this implication very seriously. The Court has expended substantial time and effort on this case. While the Court fully expects that a case of this complexity will require substantial resources and therefore is ready and willing to commit those resources to achieve a proper resolution of this matter, the Court is not willing to waste its time attempting to resolve issues that are not disputed in good faith. Thus, if Microsoft's counsel did not deem Microsoft's positions on the thirteen terms and phrases sufficiently important or well-founded to brief, they should not have presented them to the Court for consideration in the first place. Microsoft and its counsel are hereby admonished not to waste the Court's time in this or any similar way in the future.

Accordingly, the Court CONSTRUES the following terms and phrases as set out below.

a. Aspect

"Aspect" means: "Feature, element, property, or state."

b. Authentication

"Authentication" means: "Identifying (e.g., a person, device, organization, document, file, etc.). Authentication includes uniquely identifying or identifying as a member of a group."

c. Clearinghouse

"Clearinghouse" means: "A provider of financial and/or administrative services for a number of entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc."

d. Compares

"Compares" means: "Examines for the purpose of noting similarities and differences."

e. Derive

"Derive" means: "Obtain, receive, or arrive at through a process of reasoning or deduction. In the context of computer operations, the 'process of reasoning or deduction' constitutes operations carried out by the computer."

f. Designating

"Designating" means: "Indicating, specifying, pointing out, or characterizing."

g. Device Class

"Device class" means: "A group of devices which share at least one attribute."

h. Digital Signature/Digital Signing

"Digital signature" means: "A digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.)." "Digitally signing" is the process of creating a digital signature.

i. Digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class

"Digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class" means:

> Generating a digital signature (i.e., a digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.)), for the second load module, the digital signature designating (i.e., indicating, specifying, pointing out, or characterizing) that the second load module is for use by a second device class (i.e., a group of devices which share at least one attribute). The second device class must have a different tamper resistance (defined infra) or security level than the first device class.

j. Executable Programming/Executable

"Executable programming" and "executable" mean: "A computer program that can be run, directly or through interpretation."

k. Identifying at least one aspect of an execution space required for use and/or execution of the load module

"Identifying at least one aspect of an execution space required for use and/or execution of the load module" means: "Identifying an aspect (i.e., a feature, element, property, or state) of an execution space that is needed in order for the load module to execute or otherwise be used."

2. Remaining Terms and Phrases for Construction

Microsoft provided briefing on 17 of the 30 terms and phrases, as well as the issue of whether the term virtual distribution environment should be read into every claim at issue. Nevertheless, as the Court informed the parties at the mini-Markman hearing, the Court's consideration of most of Microsoft's arguments has been substantially hampered by Microsoft's persistent failure to provide evidentiary and legal citations in support of these arguments. Page after page of Microsoft's Markman Brief contains bold assertions about the meaning of certain claim terms that have few supporting authorities, and the authorities that do appear generally do not provide support for the dispositive arguments that Microsoft is asserting. (E.g., Microsoft's Markman Br. at 37, 39–40.) Without such evidentiary or legal citations, the Court has little basis to credit Microsoft's assertions.

Microsoft cannot reasonably contend that the 40 pages it was allocated for its Markman brief was insufficient for it to provide such citations, as InterTrust was able to present all of its pertinent arguments with adequate supporting citations in the 40 pages it was allocated for its opening Markman brief. Nor can Microsoft reasonably expect the Court to comb through Microsoft's voluminous submissions to locate authority that might support its specific assertions where Microsoft has failed to refer the Court to specific pages and passages in those submissions. Nor could Microsoft reasonably expect to be able to raise new arguments or cite to new authorities for the first time at the mini-Markman hearing, other than to respond to arguments or authorities appearing for the first time in InterTrust's reply brief. As far as the Court is concerned, the persuasiveness of an argument in support of a proposed construction is in direct proportion to the authorities on which it is premised. Necessarily this means that an argument that lacks appropriate supporting citations is no argument at all. Thus, Microsoft cannot be heard to complain that the Court has not adequately considered its arguments where these arguments are insufficiently supported by citations to evidentiary and/or legal authorities.

With the foregoing in mind, the Court turns to its consideration of the 17 terms and phrases briefed by Microsoft, the two terms and phrases not construed above, and the "global construction" of virtual distribution environment asserted by Microsoft.

a. Global Construction of Virtual Distribution Environment (VDE)

At the outset, there is some uncertainty over Microsoft's position about the global

United States District Court
For the Northern District of California

construction of virtual distribution environment ("VDE"). In Exhibit A to the JCCS, Microsoft indicates that its position is that each of the seven claims at issue in this mini-Markman proceeding should be construed to incorporate a VDE. More specifically, Microsoft states with respect to nine of the twelve claims: "Claim as a whole: The recited method is performed within a VDE." (JCCS Ex. A at 1 (¶ 1), 9 (¶ 14), 11 (¶ 25), 13 (¶ 38), 20 (¶ 65), 26 (¶ 74), 28 (¶ 81), 36 (¶ 98), 39 (¶ 110) (underscoring in original) (boldface omitted).) Microsoft offers similar pronouncements with respect to the remaining three claims. (See id. at 15 (¶ 51), 24 (¶ 70), 30 (¶ 86).) Further, Microsoft asserts the following in its Markman brief:

> The claims must be read in light of the entire 900+ page "Big Book" patent application and, in particular, its 115 page "Summary of the Invention." This Summary of the Invention makes literally hundreds of statements touting the "important," "fundamental," "critical," and required features, capabilities and purposes of the "present invention." The Summary further defines this "invention" (which it expressly names "VDE") by distinguishing it from the allegedly "limited" and rigid solutions of others. All of these are required aspects of the "present invention," not merely optional features of a "preferred embodiment." As such, the claims must be read to include these "invention" features.

(Microsoft's Markman Br. at 1 (emphasis added).) Microsoft states elsewhere in its Markman brief that it "asks the Court to construe each claim as requiring the disclosed 'invention,' as it has been distilled in Microsoft's global 'claim as a whole' construction." (Id. at 5 (emphasis added).) It emphasizes additionally: "[T]he claim construction point being made by Microsoft is that all of these claims necessarily invoke the required 'features' of the VDE 'invention,' not that all claims require only those features. InterTrust's patent claims are free to recite additional features, which additional limitations may (or may not) make them separate 'inventions' under Patent Office restriction practice." (Id. at 15 (emphasis added).)

In its Markman briefing InterTrust purports to interpret Microsoft's position, probably as a result of these statements, to be that every claim impliedly includes a limitation of VDE—that is, there should be a global construction of VDE. (See, e.g., InterTrust's Opening Markman Br. at 7.) Microsoft does not indicate in its Markman brief that InterTrust has mischaracterized its position.

Based on Microsoft's statements in its Markman brief and JCCS and the fact that Microsoft did not take exception to InterTrust's characterization of Microsoft's position, the Court reached the same understanding of Microsoft's position that InterTrust purported to reach. At the mini-

Markman hearing, however, counsel for Microsoft claimed for the first time that InterTrust had mischaracterized its position. According to counsel, Microsoft was not contending that VDE should be read into each claim as a limitation; rather, each disputed claim term should be accorded the meaning that it has in the VDE context. (Transcript of Proceedings, Claims Construction Hearing ("Tr.") 59:2–8.)

The Court finds Microsoft's position at the mini-Markman hearing to be fundamentally different from, and not reasonably supported by, its statements in its written submissions. Microsoft repeatedly states in the JCCS that for each claim as a whole, the recited method is performed within a VDE. In addition, Microsoft states in its Markman brief that every claim must contain all features of a VDE. These pronouncements cannot be interpreted to mean anything other than that the scope of each claim is limited by all the features of a VDE. In other words, Microsoft's written statements evince the view that even if every express element of one of the claims at issue reads on an accused device, that device would still not infringe the claim if the device did not have all the features that Microsoft claims to be the hallmark of VDE. If Microsoft wished to advance the position that it presented at the hearing, it could have easily done so in its papers by stating that "each disputed claim term must be construed in accordance with its meaning in the context of VDE." At the very least, it should have alerted the Court in its Markman brief that InterTrust in its opening brief had mischaracterized Microsoft's position. Microsoft will not be heard to complain that the Court misapprehends its position where it has made affirmative representations to the Court about its position and remains silent when InterTrust purports to interpret its position consistent with those representations. The Court thus proceeds to consider the parties' arguments with the understanding that Microsoft's position is that each claim is limited by all the features of a VDE.

Microsoft contends that each claim at issue impliedly contains a limitation of VDE, even though the term VDE appears in only one of the twelve claims, 900.155, and, then, only in its preamble. The proper construction of VDE is addressed infra in Part III.B.2.t. Microsoft's argument rests on the apparent fact, which is not contested by InterTrust, that all seven of the patents-in-suit that are the subject of the mini-Markman proceeding derive from the 900-page "Big

Book" patent application submitted to the Patent Office in or about 1995.[14] Microsoft focuses on the repeated references to the "invention" and VDE in the specifications of these patents, arguing that the claims necessarily contemplate that VDE will be an additional limitation read into all the claims.

InterTrust disagrees with Microsoft's assertions, making a few key arguments. First, InterTrust points out that the eleven claims other than 900.155 contain no limitations relating to VDE. Citing a pair of Federal Circuit cases, Amgen Inc. v. Hoechst Marion Roussel, Inc., 314 F.3d 1313 (Fed. Cir. 2003), and Renishaw PLC v. Marposs Societa' Per Azioni, 158 F.3d 1243 (Fed. Cir. 1998), InterTrust argues that statements in an application regarding the invention cannot be read into the claims absent a relevant limitation in the claims themselves. (InterTrust's Opening Markman Br. at 9.) Second, citing, inter alia, Amgen, InterTrust argues that it is improper to read into claims a limitation from the specification that does not clearly and unambiguously exclude or disclaim certain embodiments. (Id. at 9–10.)

Third, InterTrust contends that specification statements about the "invention" do not limit the claims if the rest of the specification and file history do not indicate that such a limitation was intended; and InterTrust urges that several aspects of the specification and file history contradict an importation of VDE into all the claims. (Id. at 10–11.) Specifically, InterTrust points out that the PTO held that the Big Book application claimed five separate categories of invention, forcing it to restrict its application to one class of inventions to be pursued in the application. (Id. at 11–13.) InterTrust followed the PTO's command, and also filed separate "divisional" applications relating to the other categories of inventions pursuant to 35 U.S.C. § 121.[15] (Id. at 12.) In addition, InterTrust calls the Court's attention to the '876 patent, which is not one of the seven patents-in-suit that are

[14] According to Microsoft, the specification of the '193 patent publishes the Big Book specification without any substantive additions, and therefore Microsoft frequently cites to the '193 specification as a proxy for the Big Book. (Microsoft Markman Br. at 16.) InterTrust states that the '193, '891, and '912 have specifications identical to that of the Big Book, and the '900 patent is a continuation-in-part and also includes all of the text from the original application. (InterTrust's Opening Markman Br. at 12.)

[15] 35 U.S.C. § 121 provides in part: "If two or more independent and distinct inventions are claimed in one application, the Director [of the Patent and Trademark Office] may require the application to be restricted to one of the inventions. If the other invention is made the subject of a divisional application which complies with the requirements of section 120 of this title it shall be entitled to the benefit of the filing date of the original application."

the subject of the mini-Markman hearing but is one of the eleven patents-in-suit asserted by InterTrust. InterTrust explains that the '876 patent issued as a direct continuation of the Big Book application and, therefore, includes the same specification as the '193 patent, including the same statements regarding the "invention" and VDE that Microsoft has cited. (Id. at 13–14.) The '876 patent includes numerous dependent claims adding an express requirement that a process or method include a VDE. (Id. at 14.) These claims, Microsoft maintains, demonstrate that the claims do not recite a VDE, since otherwise the inclusion of the term VDE would be redundant.

Having thoroughly considered the parties' arguments in their papers and the arguments of counsel at the hearing, the Court concludes that Microsoft's position must be rejected. The PTO's determination that the Big Book application described five inventions is alone dispositive.[16] The PTO's decision makes clear that these five inventions are separate, independent, and discrete from one another, each capable of existing in the absence of the rest:

> The inventions are distinct, each from the other because of the following reasons:
>
> 2. Inventions of Groups I-V are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they shown to be separately usable. In the instant case, invention of Group I has separate utility such as protecting executable code from computer viruses. Invention of Group II has separate utility such as a computer network administration. Invention of Group III has separate utility such as protection of software. Invention of Group IV has separate utility such as a contract bidding procedure. Invention of Group V has separate utility such as auditing of pay television.
>
> 3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.
>
> 4. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

[16] The Court clarifies that, in reaching this conclusion, it needs not and does not rely on the reasoning of Rambus Inc. v. Infineon Technologies AG, 318 F.3d 1081 (Fed. Cir. 2003), a case of superficial apposition cited by InterTrust. In Rambus, the Federal Circuit found that a specific claim term should not have been read into the claims of a patent resulting from a divisional application that was filed after the PTO found that the original application claimed more than one invention. Rambus, however, is readily distinguishable because in that case the PTO specifically identified the claim term at issue and expressly defined a divisional category of inventions that excluded that claim term, see id. at 1086; the analogy here would be if the PTO had separated the five categories of inventions claimed through the Big Book based on whether or not they were limited to a VDE. Such is not the case here, and thus the Court does not rely on Rambus in considering the significance of the PTO's ruling on the Big Book.

(JCCS Ex. C at 103 (24(BB) ('193 file history, Sept. 25, 1996 Office Action at 2–3)).) The foregoing makes unequivocal that the PTO determined that the Big Book described multiple independent inventions, each with separate utility, each with separate subject matter. Given this determination, it is impossible to conclude that, as Microsoft maintains, every claim must be read to contain all the features of a single "invention," namely the "invention" allegedly described in the Big Book application.

At the hearing counsel for Microsoft invoked Netword, LLC v. Centraal Corp., 242 F.3d 1347, 1352 (Fed. Cir. 2001), for the proposition that "claims cannot enlarge what's patented beyond what the inventor described as the invention." (Tr. 62:7–10.) Counsel appropriately cited to Netword for this principle, 242 F.3d at 1347, and the Court does not disagree with its validity. But this general principle is not inconsistent with the conclusion that the Big Book application described five independent and discrete inventions and, accordingly, the Court's instant determination that each of the claims at issue should not be read to include VDE. As Netword makes clear, the focus is on what the inventor described to the PTO as the invention, not what the inventor may have subjectively believed to be the invention. Here, the inventors submitting the Big Book evidently described five separate inventions. Reading this description and reaching this conclusion, the PTO ordered the inventors to restrict their application to one of the five inventions and to pursue divisional applications if they so chose. The inventors submitting the Big Book may very well have subjectively believed that there was but a single invention, but their subjective beliefs and intent are of no moment.

The Court also finds compelling InterTrust's invocation of the '876 patent. As InterTrust notes, the '876 patent issued as a direct continuation of the Big Book application; it includes the same specification as the '193 patent. Accordingly, one would expect that Microsoft's "global construction of VDE" argument would be equally applicable to construction of the '876 patent. Indeed, as Microsoft argues in its Markman brief, "related patents should be construed consistently." (Microsoft's Markman Br. at 16.) Yet several of the claims in the '876 patent, including claims 10 through 14, expressly contain a VDE limitation. If, as Microsoft asserts, VDE should be implicitly read into all claims within all patents directly derived from the Big Book application, these claims' express VDE limitation appears redundant and nonsensical.[17]

Still further, much of Microsoft's theory for construing all the claims at issue to incorporate Microsoft's conception of VDE rests on conclusory reasoning. For example, Microsoft contends in its Markman brief:

> Contrary to InterTrust's position (InterTrust Br. at 8:9-10), all four '193 Patent mini-Markman claims concern the distribution and protection of digital content, and contemplate multiple nodes and participants. Information is received (possibly from multiple upstream content providers), then stored on a device having unspecified authorized and unauthorized users, and then conditionally transferred to another device having unspecified users. The claims promise to control three forms of unauthorized use of this distributed content: copying, distributing (to the second device), and storing (on the first and/or second device):
>
> > "if said copy control allows at least a portion of said digital file to be copied and stored on a second device...." ('193 321:10-11)
> >
> > "determining" or "determine" "whether said digital file may be copied and stored on a second device ...." ('193 321:7-9)
>
> This claim language (e.g., "if ... allows," "determining whether") is not qualified. It implies that if the copying and storing are not allowed, then they are prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made to take the unauthorized action. In other words, these claims imply that their "controls" are effective in the face of the attacks identified in the Big Book.

(Microsoft's Markman Br. at 16–17.) As InterTrust correctly notes in its reply, nothing that Microsoft has cited to the Court indicates that the claims require multiple upstream content providers, multiple users of the first device, or multiple users of the second device. (InterTrust's Reply Markman Br. at 8.) Moreover, nothing in the language from the '193 patent specification

[17] At the hearing Microsoft objected to the introduction of the text of the '876 patent in connection with the construction of the claims at issue. Microsoft contended that the '876 patent constitutes extrinsic evidence that should not be considered unless the Court finds the claim terms ambiguous. (Tr. 68:6–22.)

This objection is untimely. Microsoft had fair notice from InterTrust's Markman briefs that InterTrust was relying on the '876 patent, and it had ample opportunity to file objections to evidence prior to the hearing (as InterTrust did), yet Microsoft declined to do so. At any rate, to the extent that consideration of the '876 patent is appropriate only if the Court finds the claim terms ambiguous, this condition has been met: notwithstanding Microsoft's last-minute attempted about-face in its "global construction of VDE" position, the Court has construed that position to be that each claim must be read as containing a limitation of VDE, and this position presents an ambiguity—that each claim must implicitly contain a limitation not explicitly stated. Finally, Microsoft has effectively waived this objection by affirmatively arguing that related patents must be construed consistently. Accordingly, the Court OVERRULES this objection.

cited above implies that "if the copying and storing are not allowed, then they are prevented . . . , no matter what effort may be made to take the unauthorized action." The Court has also read the cited portion of Dr. Reiter's deposition testimony, and if fails to understand how this testimony supports this proposition. Nor does the language quoted from the '193 patent specification imply that the claims' "'controls' are effective in the face of the attacks identified in the Big Book."

Finally, as an intuitive and legal matter, the Court is wary of reading into claims a limitation that is not expressly there. As InterTrust correctly notes, "[s]pecifications teach. Claims claim." SFI Int'l v. Matsushita Elec. Corp. of Am., 775 F.2d 1107, 1121 n.14 (Fed. Cir. 1985). With its global construction argument, Microsoft is not asking for construction of a term; it is asking for wholesale importation of a term that is present in only one of the claims at issue. In the absence of substantial justification for Microsoft's position, the Court is disinclined to take such a drastic step. See Comark Communications, Inc. v. Harris Corp., 156 F.3d 1182, 1186–87 (Fed. Cir. 1998) (holding improper reading into claims a limitation appearing only in the specification).

For all of these reasons, the Court CONSTRUES the claims at issue as not impliedly incorporating the features of a VDE as a limitation.

b. Budget

InterTrust asserts that its proposed construction of the term "budget" (appearing in 193.1), "information specifying a limitation on usage," reflects the plain English meaning of the word. (InterTrust's Opening Markman Br. at 16.) In contrast, Microsoft's proposed construction of budget requires it to be a unique type of "method" that specifies a decrementable numerical limitation on future use, where "use" is defined separately. InterTrust assails Microsoft's proposal by citing examples in the specification where the terms "budget" and "BUDGET method" are used separately and arguing that, in light of these examples, budget cannot imply a method without being nonsensical. (See id.) InterTrust also portrays Microsoft's definition as being based on the preferred embodiment in the patent, and it argues that reading limitations from preferred embodiments in specifications into claims contravenes appropriate claim construction practice. (See id. at 16–17 (citing Laitram Corp. v. Cambridge Wire Cloth Co., 863 F.2d 855, 865 (Fed. Cir. 1988)).) InterTrust further adds that there is no basis in the specification to read into the definition that budget must be a decrementable numerical limitation. (Id. at 17.)

In its Markman brief, Microsoft does not present any arguments for the term budget, although it discusses the larger phrase "a budget specifying the number of copies which can be made of said digital file." (Microsoft's Markman Br. at 38–39.) Its discussion of this phrase is very brief, however: it asserts only that its construction of this phrase, which incorporates the term budget, answers the questions "can be made since when?" or "by whom?" or "by what?" (Id.)

Given Microsoft's failure to advance any argument specifically directed to its proposed definition of the term budget, the Court has no basis to adopt Microsoft's position. Moreover, the Court finds InterTrust's proposed definition of budget to be reasonable and its criticisms of Microsoft's proposal to be cogent and compelling. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES the term "budget" to mean: "Information specifying a limitation on usage."

c. A budget specifying the number of copies which can be made of said digital file

InterTrust's proposed definition of the phrase "a budget specifying the number of copies which can be made of said digital file" (193.1) uses the normal English meanings of the words, but it incorporates the separately defined terms budget and copies. (InterTrust's Opening Markman Br. at 21.) Microsoft's definition of the phrase incorporates the term budget, requires the budget to state "the total number of copies (whether or not decrypted, long-lived or accessible)," and requires that "[n]o process, user, or device is able to make another copy of the Digital File once this number of copies has been made." InterTrust criticizes the requirement that the budget state the total number of copies as unsupported by the claim term and as nonsensical. (Id.) InterTrust also contends that the requirement that no process, user, or device be able to make another copy of the digital file once the specified number of copies have been made, is inconsistent with the specification. (Id.) Microsoft responds only by claiming that its construction answers the questions "can be made since when?" or "by whom?" or "by what?" (Microsoft's Markman Br. at 38–39.)

The Court has no basis to adopt Microsoft's proposal. Microsoft does not explain why it is necessary to read into claims utilizing this phrase a limitation addressing when, by whom, or by what copies can be made of a digital file. No reason is evident. By contrast, InterTrust's definition is commonsensical. Accordingly, the Court adopts InterTrust's definition and CONSTRUES the phrase "a budget specifying the number of copies (defined infra) which can be made of said digital file" to mean: "a budget (i.e., information specifying a limitation on usage) stating the number of copies that can be made of the digital file referred to earlier in the claim."

d. Component Assembly

The parties agree that "component assembly" (912.8, 912.35) has no ordinary meaning in the art. InterTrust's proposed definition is "two or more components associated together," where components "are code and/or data elements that are independently deliverable"; InterTrust explains that component assemblies "are utilized to perform operating system and/or applications tasks." Microsoft proposes a definition that is extremely lengthy—far too long to be suitable for reproduction here.

InterTrust asserts that its proposed construction "is taken directly from the manner in which the term is used in the specification and file history." (InterTrust's Opening Markman Br. at 38.) It cites to examples in the relevant specifications. (Id. (citing JCCS Ex. C at 18 (6(A) ('193 patent at 83:12–26), 6(B) ('193 patent at 83:43–48)), 21 (6(K) ('912 patent file history, Sept. 22, 1998 Office Action at 2–3))).) InterTrust argues that certain limitations that Microsoft reads into its proposed construction are preferred embodiments, not claim elements, and this practice is improper. (Id.) It further argues that Microsoft's proposed limitation that a component assembly be assembled and executed in a "Secure Processing Environment" is directly contradicted by the specification, which states that this condition is merely an option. (Id. at 38–39.)

Microsoft's sole argument is that the only type of "component assembly" mentioned in the Big Book is the kind identified in Microsoft's proposed construction, and therefore this construction should be adopted. (Microsoft's Markman Br. at 36.) Microsoft, however, provides no citations in support of the assertion that component assembly is "uniformly" used in the Big Book to refer to executable components. (Id.) In its reply, InterTrust allows that it "did not intend to leave open the possibility that a component assembly might include no programming." (InterTrust's Reply Markman Br. at 21.) Accordingly, InterTrust states that it "is willing to amend the third sentence of its proposed construction to read as follows: 'Component Assemblies must include code, and are utilized to perform operating system and/or applications tasks.'" (Id.)

Regardless of what the Big Book says, the relevant specifications clearly contradict Microsoft's proposed construction. Moreover, Microsoft fails to provide support for all of the features of its proposed definition. InterTrust's definition, as amended above, is well-supported and reasonable, and the Court adopts it. Accordingly, the Court CONSTRUES "component assembly" to mean: "Two or more components (i.e., code and/or data elements that are independently deliverable) associated together. Component assemblies must include code, and are utilized to perform operating system and/or applications tasks."

e. Contain

The key dispute between the parties is whether "contain" (683.2, 912.8, 912.35) implies that something has within it an actual element (Microsoft's proposal), or whether it may contain either an element or a reference to the element (InterTrust's proposal). InterTrust's proposed construction is based on the plain English meaning of contain. (InterTrust's Opening Markman Br. at 27.) InterTrust further argues that its construction is consistent with the relevant specifications, which explicitly state that a container may "contain" items "without those items actually being stored within the container." (Id. at 28 (citing JCCS Ex. C at 22 (7(B) ('193 patent at 58:48–58))).) Microsoft responds in its Markman brief that such items must actually be stored in a container because Dr. Reiter testified that he could not think of any non-empty digital file that does not contain linked and/or embedded items, and thus all digital files would qualify as containers. (Microsoft's Markman Br. at 39.)

InterTrust's argument is persuasive: the language from the specifications is clear—contain includes having references. Accordingly, the Court adopt's InterTrust's proposal and CONSTRUES "contain" to mean: "To have within or hold. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found."

f. Control (n.)

InterTrust's proposed definition of the term "control" (n.) (193.1, 193.11, 193.15, 193.19, 683.2, 891.1) relies primarily on the plain English definition of the word and on the specifications. (See InterTrust's Opening Markman Br. at 17–19.) The specifications, according to InterTrust, equate control with "control information," and it provides examples of these terms that include both data and executable files. (Id. at 17–18.) InterTrust also cites to excerpts from the '193 and related file histories that suggest that a control can be a data file. (Id. at 18.) InterTrust assails Microsoft's proposed definition for requiring a control to be executable (see infra), noting that the specifications demonstrate that a control can be data, which are not executable. (Id.) InterTrust also criticizes Microsoft's proposal for requiring a secure processing environment ("SPE"), contending that the patents make clear that requiring an SPE is but a limitation in a particular embodiment, and the patents disclose an alternate embodiment known as a host processing environment. (Id.) InterTrust adds that Microsoft's requirement that control implies the ability to modify controls is but a preferred embodiment, and in any event it is a capability provided by a particular operating system described in the specification. (Id.) Finally, InterTrust objects to Microsoft's apparent application of the general definition of control to the term "user control," which, InterTrust argues, was on the parties' initial list of claim terms to be construed for the mini-Markman proceeding but was not selected. (Id. at 18–19.)

Microsoft proposes an extraordinarily lengthy definition of control that reflects the alleged use of the term in the Big Book. First, it argues that control can be explained with an analogy to a rare books library holding valuable texts, where each type of access is controlled by a different set of rules, such as a particular type of guard performing a particular function. (Microsoft's Markman Br. at 37.) Once again, Microsoft provides no citations in support of this proffered analogy. (Id.) Second, Microsoft refers to the Big Book, suggesting that the sense in which "control" is used therein should be applied to the claims at issue. (Id. at 37–38.) Third, Microsoft assails InterTrust's argument that "rules and controls" are equated with "control information," pointing out that the patent specifications distinguish between rules and controls, such as by using the phrase "rules and/or controls." (Id. at 38.)

InterTrust's arguments are generally well-supported and convincing. Microsoft's are not. The Court is not disposed to credit Microsoft's "rare books library" analogy where Microsoft has declined to take the time to provide any citations in support of it, nor will the Court accept counsel's entreaty at the hearing to divine an evidentiary basis from the sparse citations in the 36 pages appearing in Microsoft's brief before this analogy, (see Tr. 78:2–12). As for Microsoft's reliance on the Big Book, Microsoft's quotations of excerpts from the specifications demonstrate only that a control may be executable; they do not demonstrate that a control may not be non-executable. (See Microsoft's Markman Br. at 37–38.) Given that InterTrust's proposed construction allows for both executable and non-executable programming, this evidence is fully consistent with InterTrust's proposed definition.

Microsoft's only point that merits attention—a point criticizing InterTrust's proposal, not supporting Microsoft's—is its attempt to distinguish between rules and controls, and thereby its attempt to distinguish control and control information, by invoking the specifications' references to "rules and/or controls." These references to rules and controls both in the conjunctive and disjunctive may well seem to suggest that rules are distinct from controls, and thus controls cannot be equivalent to control information if, as InterTrust urges, control information is also equivalent to rules. Nevertheless, the evidentiary support cited by InterTrust is sufficient to overcome the Court's concerns. In particular, the specification for the '193 patent clearly uses control and control information interchangeably, (see JCCS Ex. C at 24 (8(C)) ('193 patent at 129:52–60)), and the file histories of the '193 patent and the '683 patent demonstrate that control is used to mean data, (id. Ex. C at 31–32 (8(W)), 32 (8(X)), 33 (8(AA))). InterTrust has thus established that control is equivalent to control information. That is the key to the Court's resolution of this issue: once this identity is established, the remaining evidence cited by InterTrust provides ample support for its position. The Court need not resolve whether "rule" has a meaning independent from control. Even if the Court were to attempt to do so, Microsoft does not provide any evidence as to what that independent meaning might be; its assertion that "[i]n the Big Book's usage, a 'rule' need not be executable, but a 'control' must be," is bereft of supporting citations. Without such evidence, the Court cannot ascribe to the phrase "rules and/or controls" a significance that would call into question the aptness of InterTrust's proposal.

Accordingly, the Court adopt's InterTrust's proposed definition and CONSTRUES "control" (n.) to mean: "Information and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required, or prevented operations, (b) the nature or extent of such operations, or (c) the consequences of such operations."

g. Controlling, Control (v.)

InterTrust asserts that "control" (v.) (193.1, 861.58) does not have any special meaning in the specifications. (InterTrust's Opening Markman Br. at 21.) Its proposed construction is based on the plain English meaning of the word: "to exercise authoritative or dominating influence over; direct." InterTrust criticizes Microsoft's proposed construction as being unduly lengthy and complex, for having no basis in the specification, and for having a particular limitation (the requirement of a VDE SPE) that is actually contradicted by the specifications. (Id. at 22.) Microsoft faults InterTrust's proposed construction as being vague and for promising only "influence" that is inconsistent with the high degree of protection that "the Blue Book promises the owners of content entrusted to VDE." (Microsoft's Markman Br. at 39.) Microsoft also advances an argument about "arbitrary granularity" that is difficult to comprehend. (Id.)[18]

InterTrust's proposed construction is consistent with the specifications. Microsoft's proposed construction does not appear to have any support in the specifications and actually contradicts them. Microsoft's reliance on the supposed promises regarding VDE contained in the Big Book is undercut by the PTO's determination that the Big Book described multiple inventions. Accordingly, the Court adopts InterTrust's sound proposal and CONSTRUES "control" (v.) to mean: "To exercise authoritative or dominating influence over; direct."

h. Controlling the copies made of said digital file

The phrase "controlling the copies made of said digital file" (193.1) appears as part of a slightly longer clause in 193.1: "and said at least one copy control controlling the copies made of

[18] Specifically, Microsoft states that "'controlling' in this 'invention' is done at an arbitrary granularity, which is an important feature that the Big Book relied upon to distinguish prior art: [¶] 'VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems)' [citation]." (Id. (citing '193 patent 275:8–11) (emphasis omitted).) Whatever the significance of this statement may be, the cited sentence from the '193 specification is inapposite because it concerns "control information," which is equivalent to the noun form of control. See supra. Here, the Court is construing the verb form of control.

said digital file[.]" InterTrust contends that this phrase is further explained by language appearing later in 193.1, namely: "if said copy control allows at least a portion of said digital file to be copied and stored on a second device." (InterTrust's Opening Markman Br. at 22.) InterTrust maintains that this further description, along with the separately defined incorporated terms, makes clear that the copy control that is controlling the copies made of said digital file, is used to determine whether a digital file may be copied to a second device. (Id.) InterTrust asserts that its definition is based on this straightforward, plain-English interpretation. (Id.)

InterTrust criticizes Microsoft's requirement of a VDE in its construction as not required by the claim and inconsistent with the specification. (Id. at 22–23.) InterTrust also assails Microsoft's definition's requirement that the copy control control "all copies of the Digital File" as not required by the claim. (Id. at 23.) Finally, InterTrust disputes Microsoft's definition's requirement that all uses and accesses be prohibited except to the extent allowed by the copy control(s). (Id.) InterTrust argues that this limitation has no support in the claim and is inconsistent with the specification, which suggests that the item may also be governed by an alternate control structure. (Id. (citing, inter alia, JCCS Ex. C at 116 (26(A) ('193 patent at 28:19–37)), 116–17 (26(B) ('193 patent at 31:29–56))).)

In its response, Microsoft does not affirmatively argue why its definition should be adopted. Rather, it faults InterTrust's definition as reading the claim more as "controlling the copying," even though the claim refers to "controlling the copies." (Microsoft's Markman Br. at 39–40.) Microsoft does not explain the significance of this distinction. (Id.) Microsoft also contends that "InterTrust's proposal suggests that the copies are transferred to the second device, but the claims recite that the file (as opposed to any copy) is transferred." (Id. at 40.) Microsoft does not cite to any authorities in support of these assertions. (Id. at 39–40.)

In its reply brief InterTrust clarifies:

> The InterTrust construction is based on the manner in which this phrase is used in the claim, in which it explains the "copy control." See JCCS Ex. A, Row 7. The nature of the copy control is further described later in the claim. JCCS Ex. A, Rows 8 and 9. InterTrust's definition is based on the phrase itself and on its context in the claim, a context Microsoft entirely ignores.

(InterTrust's Reply Markman Br. at 23.)

InterTrust's proposed construction is sensible and supported by the language of 193.1 and the '193 patent specification. Microsoft has provided no argument in support of why its proposed construction should be adopted. Accordingly, the Court adopts InterTrust's proposed construction and CONSTRUES the phrase "controlling the copies made of said digital file" for purposes of 193.1 to mean: "Determining the conditions under which a digital file may be copied (defined infra) and the copied file stored on a second device."

i. **Copy, Copied, Copying**

InterTrust's proposed construction of the term "copy"[19] and its other permutations (193.1, 193.11, 193.15, 193.19) is based on the plain English meaning of the word. (InterTrust's Opening Markman Br. at 19.) InterTrust's construction, however, requires that the copy be usable, whereas Microsoft's definition allows a copy to be ephemeral, unusable, or inaccessible. (Id.) InterTrust's proposal also allows a reproduction to involve some changes and still be a copy, as long as the essential nature of the content remains unchanged.

InterTrust maintains that the whole point of making a copy is to have it be usable; temporary, automatically-generated internal reproductions of a file by a computer do not fit this description. (See id. at 19–20.) InterTrust adds that construing copies to include such reproductions, which are copies under Microsoft's proposal, would lead to absurd results: a user attempting to utilize a budget (defined supra) by making copies could deplete the entire budget on these ephemeral reproductions without being able to use any of them. (Id. at 20.)

In advancing its proposed definition, Microsoft relies on language from the Big Book, which appears to indicate that a copy need not be usable by everyone. (Microsoft's Markman Br. at 22–23.) Microsoft contends that InterTrust's proposed construction is nonsensical because whether a file is usable and, therefore, whether it is a copy, may change depending on whether a particular user has the ability to use the file. (Id. at 23.) Finally, Microsoft argues that InterTrust's definition contravenes the VDE "invention," which, according to Microsoft, promises prevention of

[19] The parties do not distinguish between the noun form and the verb form of this word for purposes of this mini-Markman proceeding.

unauthorized copying, which may take place even if the unauthorized copier could not use the copy. (Id. at 23–24.)

The Court agrees with InterTrust that adopting Microsoft's definition of copy would lead to absurd results because a user might exhaust his entire budget by opening a file without obtaining a single usable copy—and without realizing that he was making a copy every time he opened the file. The Court cannot discern what utility might be gained from this result. At the same time, Microsoft makes a good point that once a "copy" is made, it should not cease being a copy just because it is transferred to someone else who is no longer able to use it. The Court believes that this concern is adequately addressed by adding to InterTrust's definition the requirement that the copy be usable in any way by the person, entity, or device making the copy. Thus, if a copy is made such that it is usable by the person or entity making the copy, and then it is transferred to someone else who is unable to use it, it is still a copy.

It is crucial to understand, however, that "usable" is defined broadly in this definition to mean "capable of any conceivable use," where the noun "use" has its common-English meaning. For example, if a person makes a copy of a digital file that his own computer cannot run for the purpose of e-mailing that file to a friend whose computer can run the file, the copy is still a copy: the person making the copy "used" the file by distributing it to a friend. In other words, a copy is "usable" essentially if it is accessible for any purpose. This understanding of "usable" stands in contrast to Microsoft's apparent understanding of the word. Microsoft seems to take for granted that "usable" (as used in the definition of copy) connotes a certain degree or quality of utility. For example, Microsoft's counsel at the hearing seemed to suggest that a photocopy of a Latin text made by counsel would not be usable by him because he would not be able to read it. (Tr. 221:12–222:3.) By making this assertion, counsel implicitly presumed that the copy would not be usable because it was not comprehensible by the person making the copy. But that premise is not implicit in the word "usable" as it is used in this definition. The copy, whether or not it was comprehensible by the person making the copy, would still be usable if the person making the copy had access to it and could do something with it—perhaps send it to a friend, whether or not the friend's computer could access it. Of course, if the "copy" described by counsel in his analogy fell behind the photocopy machine before the person making the copy could retrieve it and was no longer accessible, it would not be a "copy" in the sense contemplated by the claims at issue. This requirement is necessary to avoid achieving absurd results. It also illustrates the limitations of the analogy presented by Microsoft's counsel at the hearing.

Finally, the Court agrees with InterTrust that a copy need not be an exact reproduction as long as the essential nature of the content remains unchanged. Surely a user can be said to copy a music file for a song even though he only copies half the song, as long as the resulting copy retains the essential nature of the original song. And, as InterTrust's counsel explained at the hearing, (see Tr. 208:23–209:22), the same user can also be said to copy the music file even if the reproduction he generates is encrypted and thus not an exact duplicate of the original, because the reproduction retains the essential nature of the content of the original.

Accordingly, the Court adopts InterTrust's proposed definition with the aforementioned alteration, such that "copy" (v.), "copied," and "copying" are CONSTRUED to mean, respectively: "Reproduce, reproduced, reproducing, where the reproduction must be usable in any way by the person, entity, or device making the reproduction, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged." A "copy" (n.) is such a reproduction.

j. Derives information from one or more aspects of said host processing environment

InterTrust's definition of the phrase "derives information from one or more aspects of said host processing environment" (900.155) purports to rely on normal English, incorporating the separately defined terms derive, aspect, and host processing environment. (Id. at 37.) InterTrust argues that the requirement in Microsoft's proposed definition that information be derived from the host processing environment "hardware" is inconsistent with the disclosed embodiment, (id. (citing JCCS Ex. C at 129–30 (29(A) ('900 patent at 239:4–42))), and finds no support in relevant claim, 900.155, (id.). In response, Microsoft contends, without citation or clear explanation, that InterTrust's proposed construction may serve no security purpose at all because it does not require a "unique machine signature" technique allegedly identified by Dr. Reiter. (Microsoft's Markman Br.

at 40.)

InterTrust's proposed definition is sensible and supported by the '900 patent specification. Microsoft has neither provided any support for adopting its proposed definition, nor has it addressed InterTrust's arguments that certain features of its definition are inconsistent with or unsupported by the specification. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "derives information from one or more aspects of said host processing environment" to mean: "Derives (i.e., obtains, receives, or arrives at through a process of reasoning or deduction) information based on at least one aspect (i.e., feature, element, property, or state) of the previously referred to host processing environment (defined infra)."

k. Host Processing Environment (HPE)

In its opening brief, InterTrust maintains that host processing environment ("HPE") (900.155) is explicitly defined in 900.155: it consists of the elements listed in that claim. (JCCS Ex. A at 33 (¶ 87).) InterTrust maintains that HPE therefore needs no additional definition, yet it offers a definition in the alternative. (Id.) Turning to that definition, InterTrust explains it agrees with Microsoft that HPEs may be either secure or non-secure and that InterTrust's proposed definition is more accurately a definition of a secure HPE. (InterTrust's Opening Markman Br. at 36.) It therefore states that if necessary, its proposed construction should be qualified to allow for secure and non-secure HPEs, and it offers language containing such a qualification which it claims to be supported by the specification. (Id.) InterTrust, however, takes issue with Microsoft's inclusion of additional limitations in its proposed definition, arguing that they are unwarranted. For example, InterTrust points out that Microsoft's implicit assertion that an HPE consists only of executable programming contradicts 900.155, which identifies various hardware elements as part of the HPE. (Id.) Microsoft argues in response, without citations to evidence, only that the Big Book permits HPEs to be secure or non-secure, and Microsoft's proposed construction addresses this feature. (Microsoft's Markman Br. at 40.) Microsoft's proposal provides, among other things, that a secure HPE run in "protected (privileged) mode" and that a non-secure HPE run in "user mode."

At the hearing the Court explored InterTrust's offer to qualify its original proposed definition. InterTrust's counsel proposed that the proffered definition be modified to the following:

United States District Court
For the Northern District of California

"[A] host processing environment may be either secure or non-secure. A secure host processing environment is a protected processing environment incorporating software-based security, and a non-secure host processing environment is a processing environment with insufficient security to constitute a secure host processing environment." (Tr. 264:19–24.) Counsel, however, adhered to the position that the Court need not define this term because it consists of the elements of 900.155. (Tr. 265:22–266:14.) Counsel contended that the reference to HPE in 900.155 is similar to a preamble, requiring no construction by the Court, but he admitted that he could not cite to the Court any authority in support of this position. (Id.) Microsoft's counsel responded to InterTrust's amended proposal by arguing that it was nonsensical to construe HPE to include both secure and non-secure processing environments because an HPE is a type of protected processing environment. (Tr. 268:21–269:12.) He cited portions of the '193 patent specification in support of this position. (Tr. 269:18–271:10.) Microsoft's counsel admitted, however, that Microsoft's own proposed definition allowed for HPE to be both secure and non-secure. (Tr. 273:21–274:1.) InterTrust's counsel commented that the key difference between InterTrust's revised proposal and that of Microsoft was that Microsoft's proposal requires that an HPE run in protected mode. (Tr. 272:12–14.) He went on to assert that there is no statement in the '193 patent that suggests that a secure HPE or a non-secure HPE must operate in a particular mode. (Tr. 272:15–273:7.)

The Court fully understands InterTrust's position that the reference in 900.155 to HPE is akin to a preamble requiring no construction, as that reference appears on the second line of the claim without any other elements. Yet given the references to HPE in conjunction with protected processing environments and secure processing environments in the specifications of the '193 patent and the '900 patent, (JCCS Ex. C at 56 (16(B) ('193 patent at 105:18–22, '900 patent at 112:48–52))), the Court considers it to have significance independent from the remaining elements of 900.155 themselves. The Court thus construes HPE accordingly.

Microsoft's proposed definition is not plausible. Microsoft provides no support for the requirement that HPE be "within a VDE node" or for the requirement that a secure HPE run in protected mode and a non-secure HPE run in a different mode. InterTrust's revised proposal, on the other hand, properly incorporates the term "protected processing environment" (defined infra) consistent with HPE's use in the specifications. Moreover, the Court does not agree with Microsoft's suggestion that InterTrust's proposed definition is nonsensical because there cannot be a non-secure protected processing environment. A protected processing environment is a separately defined term that, under InterTrust's proposed definition, provides protection against tampering. (See JCCS Ex. B at 11 (¶ 18).) InterTrust's proposed definition of tampering (a term that is not offered for construction by the Court but will be implicitly defined in the Court's construction of "tamper resistance") is not coextensive with its proposed definition of secure. (Compare id. Ex. B at 15 (¶ 21) with id. Ex. B at 13 (¶ 19).) Given that, as discussed infra, the Court adopts InterTrust's proposed definitions of secure and tamper resistance, there is no inconsistency in concluding that HPEs may be secure and non-secure. Moreover, Microsoft's own proposed construction of HPE allows it to be either secure or non-secure.

Accordingly, the Court adopts InterTrust's revised proposal and CONSTRUES "host processing environment" (and its acronym, "HPE") as follows: "A host processing environment may be either secure or non-secure. A secure host processing environment is a protected processing environment (defined infra) incorporating software-based security, and a non-secure host processing environment is a processing environment with insufficient security to constitute a secure host processing environment.

l. Identifier

InterTrust contends that its proposed construction of "identifier" (193.15, 912.8) is based on the normal English meaning of the term and is consistent with its use in the specifications. (InterTrust's Opening Markman Br. at 24.) InterTrust asserts that the main dispute between the parties is whether, as Microsoft contends, identifier must be unique to an "individual instance" of a person or thing, or whether, as InterTrust contends, it can specify that a person or thing is a member of a group. (Id.) InterTrust points to a specification embodiment of a portion of 912.8 that appears to lend support to its construction. (Id. (citing JCCS Ex. C at 131 (30(A) ('193 patent at 140:15–46))).) Microsoft in response does not address identifier, but rather "identifying (identify)." (Microsoft's Markman Br. at 40.) Without offering any evidentiary citations in support, Microsoft asserts that "[i]n common usage and these patents, to identify someone or something is to establish the person or thing as a particular individual or thing." (Id.) In its reply brief, InterTrust objects to Microsoft's construction of the terms "identifying (identify)", contending that they are distinct from identifier and were not agreed-upon as terms that would be construed at the mini-Markman. (InterTrust's Reply Markman Br. at 23 n.13.) InterTrust adds that its proposed construction is based on the American Heritage Dictionary. (Id. at 23.)

InterTrust's arguments are persuasive. Microsoft's argument is unsupported. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "identifier" to mean: "Information used to identify something or someone (e.g., a password). In this definition, 'identify' means to establish the identity of or to ascertain the origin, nature, or definitive characteristics of; includes identifying as an individual or as a member of a group."

m. Protected Processing Environment (PPE)

InterTrust contends that its proposed construction of "protected processing environment" ("PPE") (683.2, 721.34) is consistent with the specifications, which describe two embodiments of a PPE: a secure processing environment ("SPE") and a host processing environment ("HPE"). (InterTrust's Opening Markman Br. at 28–29.) InterTrust explains that its construction properly covers both embodiments because the specification explicitly states that any action that can be taken by an SPE can also be taken by an HPE, albeit possibly with a lower level of security. (Id. at 29.) InterTrust further contends that a number of Microsoft's proposed definitions would improperly exclude the HPE embodiment, which provides software-based security. (Id.) InterTrust adds that Microsoft's proposed definition of PPE is 345 words in length and thus impossible for any jury to understand. (Id.)

In its Markman brief Microsoft address only what it deems to be the "central dispute": whether a PPE must have a physical tamper resistant barrier (see infra) and prevent unauthorized access, observation, and interference. (Microsoft's Markman Br. at 34.) Although Microsoft's discussion of issues relating to the proper construction of PPE runs a page and a half in length, careful review of this discussion reveals only one substantive argument in support of its proposed definition: that the three reasons provided elsewhere in the brief for adopting Microsoft's construction of tamper resistant barrier also demonstrate that these claims' PPE must be the hardware-based SPE, not the software-based HPE. (Id. at 35.) Microsoft also faults InterTrust's proposed definition as being "vague" and lacking in more specific information. (Id.)

InterTrust's arguments are persuasive and well-supported. Given that, as discussed infra, Microsoft's tamper resistant barrier arguments are unavailing, so, too, are its arguments regarding PPE. Further, InterTrust's proposed definition is not vague, and Microsoft does not demonstrate that the information that is not provided in InterTrust's definition is crucial. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "protected processing environment" to mean: "An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat. In this definition, 'environment' means capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network)."

n. Secure, Securely

InterTrust's proposed construction of "secure" and "securely" (193.1, 193.11, 193.15, 683.2, 721.34, 861.58, 891.1, 912.8, 912.35) is flexible and denotes any of several different attributes, including secrecy and authenticity, some or all of which may be applicable depending on the particular context discussed in the specifications. (See InterTrust's Opening Markman Br. at 14–16.) InterTrust assails Microsoft's proposed definition, which requires all of five qualities identified by Prof. Mitchell, as being flatly contradicted by the specifications, which in some contexts make clear that secure connotes fewer than all five of these qualities. (See, e.g., id. at 14 (quoting '193 patent at 233:25–30 ("In one embodiment, the portable appliance 2600 could support secure (in this instance encrypted and/or authenticated) two-way communications with a retail terminal which may contain a VDE electronic appliance 600 or communicate with a retailer's or third party provider's VDE electronic appliance 600.")); see also id. at 14–15.) InterTrust asserts that, as Dr. Reiter has testified, nothing is absolutely secure; InterTrust maintains that its proposed construction reflects this reality, whereas Microsoft's does not. (See id. at 15.)

Microsoft's proposed definition requires that something must have all five of the following qualities to be secure: "availability"; "secrecy"; "integrity"; "authenticity"; and "nonrepudiation."

(Microsoft's Markman Br. at 28.) Microsoft contends that its definition "honors the basic premise of VDE." (Id. at 27.) Microsoft provides no citations whatever in support of its proposal, other than certain extrinsic evidence tending to suggest that secure connotes an absolute state. (Id. at 25–28.) Microsoft criticizes InterTrust's proposal on several grounds (without citations), one of which is that InterTrust's definition, which contains the phrase "one or more mechanisms are employed to . . .", suggests that something can be secure simply if an effort is made, regardless of the result; Microsoft maintains that the term secure connotes a state, regardless of the effort made to achieve that state. (Id. at 26.)

The Court finds InterTrust's proposed definition, for the most part, to be very well supported by the relevant specifications. Microsoft's definition, by contrast, has no evidentiary support and is, in fact, clearly contradicted by the specifications of the patents-in-suit.

But there are a few modifications to InterTrust's proposal that the Court explored with the parties at the hearing and that the Court now deems appropriate to make. First, Microsoft makes a good point that secure connotes a state—albeit not necessarily an absolute state—and not merely an effort. Thus, InterTrust's use of the phrase "one or more mechanisms are employed to . . ." in its proposed construction is potentially problematic. To address this concern, the Court proposed at the hearing modifying this phrase to "one or more mechanisms are employed that . . . ." This alteration indicates that a state has been achieved, not merely that an effort has been made. InterTrust's counsel stated at the hearing that InterTrust had no objection to this modification. (Tr. 121:18–122:1, 149:24–150:1.) Nevertheless, the Court recognizes that a particular mechanism may not by itself prevent, discourage, or detect misuse; rather, it may do so only in conjunction with other mechanisms. Accordingly, the Court believes that a further modification would be helpful: the phrase should read "one or more mechanisms are employed that (whether alone or in conjunction with one or more other mechanisms) . . . ."

Second, the Court agrees with Microsoft's proposal at the hearing—a proposal that counsel later withdrew—that the portion of the last sentence of InterTrust's proposal, namely "but is designed to be sufficient for a particular purpose", should be stricken, such that the sentence shall read: "Security is not absolute." (Tr. 148:14–149:21, 152:20–153:3.) This proposal arose out of the debate between counsel for InterTrust and counsel for Microsoft about whether something can be secure if it does not guarantee protection against specified threats. Although the Court fully appreciates the distinction that the parties have sought to draw, the Court agrees with InterTrust that security is not absolute and that the language in question adds nothing to the definition and might confuse to a jury. The statement that "security is not absolute" fully captures the meaning sought to be conveyed. Moreover, Microsoft's counsel agreed at the hearing that security is not absolute, (Tr. 141:22 ("So we agree secure is not absolute . . . ."), 152:24 ("[S]aying 'secure is not absolute' . . . [is] a truism . . . ."), and InterTrust's counsel represented that InterTrust was amenable to this modification, (Tr. 149:8–24).

Finally, the Court agrees with Microsoft's concern that defining secure to include mechanisms that merely detect misuse of or interference with information or processes is inappropriate. At the same time, it is clear that the relevant claims contemplate employing security technologies including digital signatures. (See JCCS Ex. C at 74 (19(A)) (citing '193 patent at 8:1–3).) As explained to the Court at the hearing, digital signatures do not provide security by preventing or discouraging misuse of data; instead, they provide security by alerting the user to misuse or interference with the data in question, thereby allowing the user to avoid harm stemming from the misuse or interference. It would thus be inappropriate to exclude detection from the definition of security altogether. The Court believes that it can accommodate Microsoft's concerns while remaining faithful to the meaning of secure contemplated by the patent specifications by modifying "detect" in InterTrust's proposal to "detect misuse of or interference with information or processes for the purpose of discouraging and/or avoiding harm."

Accordingly, the Court adopts InterTrust's proposed definition with the modifications stated above and CONSTRUES "secure" to mean:

///

///

///

///

///

> One or more mechanisms are employed that (whether alone or in conjunction with one or more other mechanisms) prevent or discourage misuse of or interference with information or processes, or that detect misuse of or interference with information or processes for the purpose of discouraging and/or avoiding harm. Such mechanisms may include concealment, tamper resistance (defined infra), authentication (i.e., identifying (e.g., a person, device, organization, document, file, etc.)), and access control. Concealment means that it is difficult to read information (e.g., programs may be encrypted). Tamper resistance and authentication are defined separately. Access control means that access to information or processes is limited on the basis of authorization. Security is not absolute.

"Securely" means: "In a secure (defined supra) manner."

o. Secure Container

InterTrust's proposed construction of "secure container" (683.2, 861.58, 912.35) is straightforward: a container (defined supra) that is secure (defined supra). InterTrust provides several examples from the specifications that support its proposed construction. (InterTrust's Opening Markman Br. at 26 (citing, inter alia, JCCS Ex. C at 83 (20(A) ('193 patent at 127:30–49)), 84 (20(C) ('683 patent at 15:61–16:4))).) InterTrust also takes issue with a number of features of Microsoft's proposed definition, arguing, inter alia, that it conflicts with the specifications, (id. at 26), that it impermissibly relies on the preferred embodiment, (id. at 27), and that one of its limitations finds no support in the specifications or elsewhere, (id.).

Microsoft proposes a construction of secure container that is enormous in length. Microsoft relies almost exclusively on the alleged Big Book's description of a VDE secure container. (See Microsoft's Markman Br. at 29.) The crucial feature of this proposed type of container is that it prevents, and not simply detects, all access to and use of protected content—i.e., it promises absolute protection. (Id. at 30 ("This 'access control' ability of VDE secure containers is critical to VDE's promise to content owners that it can prevent (not simply detect) all access to and use (not just decryption-based uses) of protected content.").)

InterTrust responds that one feature contained in Microsoft's definition, namely that a secure container includes an access control method, is but an example of an embodiment in the specifications, not the only embodiment disclosed. (InterTrust's Reply Markman Br. at 18.) InterTrust adds that the term "VDE secure container" does not appear anywhere in the '193 patent; when the inventors of that patent wanted to refer to a container in terms of VDE capabilities, they used the term "VDE container." (Id. at 19.) InterTrust presents examples of the use of the term VDE container. (Id. at 19.)

InterTrust's proposed construction is well-supported by the specifications. Microsoft's proposed construction, which relies on the concept of a VDE secure container, is contradicted by the specifications, as InterTrust demonstrates. In addition, as InterTrust's counsel pointed out at the mini-Markman hearing, Microsoft's counsel's reference to the '193 patent specification in support of its assertion that a VDE container is equivalent to a secure container is misleading: the portion of the specification cited by Microsoft refers only to the preferred embodiment. (Tr. at 238:10–239:11, 240:22 (discussing '193 patent at 127:40–50).)[20] As discussed supra, it is inappropriate for the Court to read limitations in the preferred embodiment into the claim terms. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "secure container" to mean: "A container (defined supra) that is secure (defined supra)."

p. Securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item

The phrase "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item" appears only in 891.1. InterTrust contends that "securely applying" is not specially defined in the specification and is not a term of art. (InterTrust's Opening Markman Br. at 34.) InterTrust explains that in the specification, the terms "securely applying" and "applying" refer to the application of control information to govern content. (Id. (citing, inter alia, JCCS Ex. C at 126 (28(A) ('193 patent at 299:19–51))).) InterTrust faults several features of Microsoft's proposed definition for being inconsistent with the specification and/or for lacking support in the specification. (See id. at 34–35.) Microsoft proposes a lengthy definition for this phrase, but it has elected not to address this phrase in its Markman brief.

InterTrust's proposed definition, at least to the extent it relies on a construction of "securely applying" or "applying," has support in the specification. Microsoft has presented no reason to

[20] The Court needs not even consider this portion of the '193 specification because Microsoft never cited to it in its Markman brief.

adopt its proposed definition. Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item" to mean: "The first entity's control (defined supra) and the second entity's control are securely (defined supra) applied to govern use (defined infra) of the data item, the act of securely applying involving use of the resource."

q. Tamper Resistance

InterTrust advances a construction of "tamper resistance" (721.1) that, it contends, is consistent with the use of the term in the specifications and in relevant extrinsic evidence. (InterTrust's Opening Markman Br. at 31.) InterTrust faults Microsoft's proposed definition as requiring that access, observation, and interference be prevented; InterTrust contends that this requirement is inconsistent with the plain meaning of "resistance." (Id.) InterTrust also faults Microsoft's definition as inexplicably requiring prevention of access, which is not connoted by the term "tampering." (Id.)

Microsoft presents little in the way of argument in support of its proposed definition. Microsoft faults InterTrust's definition as failing to specify with what is being compared in connection with the phrase "making tampering more difficult." (Microsoft's Markman Br. at 40.) It also states that "merely detecting tampering but not stopping it, plainly is not what VDE means by 'tamper resistance.'" (Id.) It does not provide any evidentiary or legal citations in support of these statements. (Id.) InterTrust replies in succinct fashion: it states that tamper resistance makes tampering "more difficult" to achieve than it is to achieve in the absence of tamper resistance; and it points out that Microsoft's unsupported assertion about what VDE means by tamper resistance is not evidence supporting Microsoft's construction. (InterTrust's Reply Markman Br. at 24.)

InterTrust's citations to intrinsic evidence, namely the patent specifications, are sufficient to demonstrate that its proposed construction is correct. (See JCCS Ex. C at 87 (21(A) ('721 patent at 4:40–42); 21(B) ('193 patent at 59:48–59)).) Reference to the extrinsic evidence that InterTrust offers is not necessary, although the Court notes that that evidence clearly supports InterTrust's proposed construction. (See, e.g., id. Ex. C at 88 (21(D) (quotation from text on tamper resistant software that defines such software as "software which is resistant to observation and modification")).) By contrast, Microsoft provides no citations whatever in support of its proposal. There is therefore no basis on which the Court can adopt Microsoft's definition. Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "tamper resistance" to mean: "Making tampering more difficult and/or allowing detection of tampering. For purposes of this definition, 'tampering' means using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use."

r. Tamper Resistant Barrier

InterTrust's proposed definition of "tamper resistant barrier" (721.34) is straightforward: "hardware and/or software that provides tamper resistance." InterTrust contends that its definition is consistent with the use of the term in the specification. (InterTrust's Opening Markman Br. at 32–33 (citing JCCS Ex. C at 90 (22(C) ('721 patent at 5:1–6))).) InterTrust further contends that, in accordance with the specifications, its definition permits a tamper resistant barrier to consist of hardware or software. (Id. at 33 (citing JCCS Ex. C at 89–90 (22(B) ('193 patent at 80:22–65))).)

Microsoft claims that its definition, which requires a hardware device and which requires prevention of unauthorized access, observation, and interference, is based on the underlying premise of VDE in the Big Book. (Microsoft's Markman Br. at 30–33.) Microsoft also faults InterTrust's definition of tamper resistant barrier, which incorporates the defined term tamper resistance, as failing to answer the questions "'making tampering more difficult' than what?" and "[w]hat does 'allowing detection of tampering' mean?" (Id. at 34.)

InterTrust points out in its reply that Microsoft's definition's requirement that a tamper resistant barrier include a physical hardware device is contradicted by an express embodiment disclosed in the specification. (InterTrust's Reply Markman Br. at 5–6.) InterTrust states that it "is aware of no Federal Circuit case that has ever held that a claim term can be interpreted to exclude, not merely a disclosed embodiment, but a disclosed embodiment that is identified in the specification using exactly the same words as the claim ('tamper resistant barrier')." (Id. at 6 (emphasis in original).) InterTrust adds that the term is found only in 721.34, and this term contains no reference to assigning usage control information or any use of content, nor does it have any language from which such elements can be inferred, yet Microsoft's definition includes such elements. (Id. at 19.)

The Court agrees with InterTrust that Microsoft's proposed definition cannot be correct, since it contradicts the use of the term in an embodiment expressly disclosed in the relevant specifications. Indeed, language from one of the specifications that Microsoft itself cites demonstrates that a tamper resistant barrier may consist of software alone: Microsoft quotes from the '900 patent text that includes the following sentence: "No software-only tamper resistant barrier 674 can be wholly effective against all of these threats." (Microsoft's Markman Br. at 33 (quoting from '900 patent at 233:24–33) (emphasis added).) Obviously, the specification contemplates that a tamper resistant barrier may be software-only; such a software-only tamper resistant barrier, however, will not be wholly effective against all the threats identified. Had the inventors intended to exclude software-only mechanisms or processes from the definition of tamper resistant barrier, they would have said something to the effect of "no software-only mechanisms or processes can be a tamper resistant barrier because they cannot be wholly effective against all of these threats." Similarly, Microsoft's quotations of certain portions of specifications in support of its definition demonstrate only that a tamper resistant barrier may be a hardware device under the appropriate circumstances; but these quotations do not demonstrate that it must be a hardware device. (See, e.g., id. (quoting '193 patent at 49:15–17) ("A hardware SPU (rather than a software emulation) with a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required."); see also id. at 32–34.) Finally, Microsoft's practice, utilized frequently in its discussion of other claim terms and phrases, of faulting InterTrust's proposed definition for not addressing certain questions, (id. at 34), is unconvincing because there is no evidence that it is even necessary to address these questions.

Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "tamper resistant barrier" to mean: "Hardware and/or software that provides tamper resistance (defined supra)."

s. Use

InterTrust contends that the term "use" (193.19, 683.2, 721.1, 861.58, 891.1, 912.8, 912.35) is not specially defined in the specification, and it is not a term of art. (InterTrust's Opening Markman Br. at 25.) InterTrust's proposed construction is based on the plain English meaning of the word use: "to put into service or apply for a purpose, to employ." (Id.) Microsoft's proposed construction appears similar, but it provides examples of the term use (e.g., copying, printing, decrypting) and requires an additional limitation pertaining to VDE. (See Microsoft's Markman Br. at 20–21.) Yet Microsoft does not clearly explain in its Markman brief how the first part of its proposed definition—"[t]o use information is to perform some action on it or with it"—is inconsistent with InterTrust's proposed definition, nor does it clearly explain the basis for the second part of its proposal, which imposes an additional limitation relating to VDE.

At oral argument the Court expressed its uncertainty regarding Microsoft's position in these two respects. Counsel for Microsoft informed the Court that it would be a "reasonable approach" for the Court to take if it struck out the second part of its proposed definition (the portion pertaining to VDE). (Tr. at 228:9–12.) As for the first part of its proposed definition, Microsoft's counsel stated that its proposed definition was intended only to provide examples of "use" for the jury to better understand the term in the sense Microsoft intended. (See Tr. 224:18–14, 227:8–228:8, 229:7–22.)

The Court discerns insufficient support for the second part of Microsoft's proposal, and in light of Microsoft's willingness to excise it, the Court agrees that this part is not due serious consideration. As for the first part of Microsoft's proposal, the Court believes that providing the examples of the term use that Microsoft has listed adds nothing in the way of clarification to the definition of the term and may in fact confuse the jury. Specifically, Microsoft does not indicate that these examples are exhaustive or that they have a particular relationship. Thus, a jury will be required to guess at their significance to determine what limiting purpose they serve, if any. At the same time, InterTrust's definition is more straightforward and is in fact consistent with this first portion of Microsoft's proposed definition.

Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "use" to mean: "To put into service or apply for a purpose, to employ."

t. <u>Virtual Distribution Environment (VDE)</u>

InterTrust points out that among the twelve claims at issue in the mini-Markman proceeding, the term "virtual distribution environment" ("VDE") (900.155) appears only in the preamble of 900.155. (InterTrust's Opening Markman Br. at 35.) It argues that the individual elements of 900.155 fully define the recited apparatus, and reference to the preamble is not necessary to define and understand the claimed apparatus. (Id.) Citing Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1371 (Fed. Cir. 2003), and Alfred J. Schumer v. Laboratory Computer Systems, Inc., 308 F.3d 1304, 1310 (Fed. Cir. 2002), InterTrust contends that the preamble does not "give life, meaning and vitality" to the claim, and therefore it is irrelevant to claim interpretation. (InterTrust's Opening Markman Br. at 35.) Accordingly, InterTrust asserts that VDE need not be defined and should not be read into claims that do not actually recite it. (See id.)

Without waiving its position that VDE should not be read into claims that do not actually recite it, InterTrust argues that to the extent it must be defined, the Court should adopt the short definition that it proposes, which is taken directly from embodiments of VDEs described in the specification. (Id.) InterTrust faults Microsoft's proposed definition, which consists of over 2,000 words, as incomprehensible by a lay jury. (Id.) It further criticizes Microsoft's proposed definition's requirement of a "secure processing environment" embodiment as conflicting with the specification's clear description of an alternate embodiment HPE. (Id.) It adds that, given that Microsoft seeks to read VDE into each and every claim, the "universe-wide" feature of VDE required in Microsoft's definition would appear impossible to apply to a claim relating to a single device or process. (Id. at 35–36.) It also insists that the requirements in Microsoft's definition that a VDE "guarantee" various types of security and that a VDE be "non-circumventable" is inconsistent with the real-word fact that guaranteed security is impossible, and it is inconsistent with the specification. (Id. at 36.)

Microsoft proposes a definition that is nothing short of gargantuan in length. Its proposed definition purports to be derived from numerous statements in the Big Book application. (See Microsoft's Markman Br. at 3–9.) Microsoft does not address InterTrust's contention that VDE should not be defined separately from the elements of 900.155 because it is found in the preamble and arguably does not give "life, meaning, or vitality" to the claim.

The Court agrees with InterTrust that VDE does not require construction independent of the elements of 900.155. The Court cannot possibly discern what "life, meaning, or vitality" VDE imbues in the claim. The claim terms speak for themselves. Moreover, the Court has difficulty accepting Microsoft's proposed definition of VDE to the extent it purports to be premised on the Big Book application where, as discussed supra, the PTO determined that the Big Book described five different inventions. Finally, given that the Court has stricken the Maier Declaration, the Court has no evidentiary basis to conclude that VDE would be construed by a person of ordinary skill in the art in the manner that Microsoft suggests. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "virtual distribution environment," as that term appears in 900.155, to be defined by the elements of 900.155; it has no definition independent of those elements.

IV. CONCLUSION

Despite its misgivings, the Court agreed to conduct this mini-Markman proceeding and resolve Microsoft's motion for summary judgment on indefiniteness at this stage of the litigation based on the parties' representations that early resolution of these matters would facilitate compromise. The Court also agreed to enter the partial stay of this action on Microsoft's request based on Microsoft's representations that proceeding with this litigation full-throttle might prove unnecessary if the Court would construe a key subset of claim terms and phrases and resolve certain other issues in dispute. To these ends the Court has expended tremendous time and effort.

Microsoft's decision to ignore approximately 40 percent of the claim terms and issues which were selected by the parties and its failure to provide substantial citations to evidentiary and legal authorities in support of its positions call into question the prudence of the Court's having proceeded in this fashion. It also lends credence to the suggestion that Microsoft's purported opposition to many of InterTrust's proposed constructions is baseless, and it implies that to a large extent the eight-month delay in this case has been for naught. It was Microsoft, after all, that proposed that thirty claim terms and phrases should be construed in this proceeding, arguing in a submission to the Court that construction of this many terms and phrases "should suffice to cover the most important disputes." That Microsoft evidently felt entitled to multiply the proceedings needlessly is more than a little disconcerting.

United States District Court
For the Northern District of California

The Court expects the parties now to conduct compromise negotiations earnestly and in good faith, as would be expected by their earlier representations to the Court. In the meantime, the Court wishes to make the following unequivocal: The Court will not tolerate a party's creating a dispute by taking a position on a material issue where that party does not have a good-faith basis for that position that is well-supported by fact and by law. Such conduct may result in the imposition of sanctions under Federal Rule of Civil Procedure 11 and/or other authority that may be applicable. Microsoft should be aware that this instruction applies with special force to it in light of its objectionable performance in the instant proceedings.

Accordingly,

IT IS HEREBY ORDERED THAT:

1. Microsoft's Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness [Docket No. 229] is DENIED.

2. Claims 193.1, 193.11, 193.15, 193.19, 683.2, 721.1, 721.34, 861.58, 891.1, 900.15, 912.8, and 912.35 are CONSTRUED as set forth in the body of this Order.

3. Consistent with the parties' representations to the Court in their joint letter dated June 26, 2003, and the Court's consideration thereof, **no later than July 9, 2003,** the parties shall file with the Court a joint statement of any reasonable length explaining whether the parties have obtained the consent of an Article III Judge of the Northern District of California to conduct settlement discussions (and if so, which Judge), and if not, what, if anything, the parties would like the Court to do to assist in their conducting settlement discussions. The Court will issue an appropriate Order shortly thereafter pertaining to such settlement proceedings.

4. The parties shall **telephonically** appear at a Case Management Conference before the Court on **August 7, 2003, at 3:~~15~~ 30 p.m.** InterTrust's counsel shall set up the **telephonic** conference call with all the parties on the line and call chambers at (510) 637-3559 at the time designated above. **NO PARTY SHALL CONTACT CHAMBERS DIRECTLY WITHOUT PRIOR AUTHORIZATION OF THE COURT.** The parties shall file a Joint Case Management Statement at least ten (10)

days prior to the conference.

IT IS SO ORDERED.

Dated: July 3, 2003

Saundra B. Armstrong
SAUNDRA BROWN ARMSTRONG
United States District Judge